MATH 204 Notes

March 14, 2013

1 Absolute values

1.1 Generalized absolute values

Let F be a field.

Definition 1.1. An *absolute value (norm)* on F is a map $|\cdot| : F \to [0, \infty)$ with the following properties:

(i) $|ab| = |a||b|$ for all $a, b \in F$;

(ii) $|a| = 0 \iff a = 0$;

(iii) $|a + b| \leq |a| + |b|$ for all $a, b \in F$.

Example 1.2. These are all well-known prototypes.

1. the usual absolute value on $\mathbb{Q}$
2. the usual absolute value on $\mathbb{R}$
3. the usual absolute value on $\mathbb{C}$

Example 1.3. The *trivial absolute value* $|a| = 1$ for all $a \in F^\times$.

Definition 1.4. Assume $|\cdot|$ is an absolute value on the field F. A *norm (compatible with $|\cdot|$)* on an F-vector space V is a map $\|\cdot\| : V \to [0, \infty)$ with the following properties:

(i) $\|ax\| = |a|\|x\|$ for all $a \in F, x \in V$;

(ii) $\|x\| = 0 \iff x = 0$;

(iii) $\|x + y\| \leq \|x\| + \|y\|$ for all $x, y \in V$.

Example 1.5. The Euclidean norm on $\mathbb{R}^n$ or $\mathbb{Q}^n$ or $\mathbb{C}^n$ is a norm compatible with the usual absolute value on the relevant field. Same for other norms from analysis, like the sup norm.

Example 1.6. The L^2 norm on the space of square-integrable functions on $\mathbb{R}^n$. Similarly, the L^1 norm on the space of integrable functions or the L^p norms (here $1 < p \leq \infty$.)

Example 1.7. The operator norm on the space of $m \times n$ matrices over $\mathbb{C}$, given by

$$\|A\| = \sup\{\|Ax\|; x \in \mathbb{C}^n, \|x\| \leq 1\}.$$

Definition 1.8. A *generalized absolute value* on a field F is a map $|\cdot| : F \to [0, \infty)$ with the following properties:

(i) $|ab| = |a||b|$ for all $a, b \in F$;

(ii) $|a| = 0 \iff a = 0$;

(iii) there exists a constant $C > 0$ such that $|a + 1| \leq C$ for all $a \in F$ with $|a| \leq 1$.

The last condition is called the *weak triangle inequality.* It implies that

$$|a + b| \leq C \max\{|a|, |b|\} \leq C(|a| + |b|).$$

Example 1.9. The square of the usual absolute value on $\mathbb{C}$ is not an absolute value, but it is a generalized absolute value.

Remark 1.10. *The multiplicativity* (i) *in the definition of a generalized absolute value on a field* F *is much stronger than the corresponding property of a norm on a vector space.*

Lemma 1.11. *If* $|\cdot|$ *is a generalized absolute value on the field* F, *then*

(i) $|1| = |-1| = 1$

(ii) $|-a| = |a|$ *for any* $a \in F$

(iii) $|a^{-1}| = \frac{1}{|a|}$

(iv) *if* $|a^n| = 1$ *for some* $a \in F, n \neq 0$ *then* $|a| = 1$.

Proof. Exercise! □

Proposition 1.12. *The only generalized absolute value on a finite field* F *is the trivial one.*

Proof. For any $a \in F^\times$ we have $a^q = 1$ where q denotes the number of elements in F. By the previous Lemma, this implies that $|a| = 1$. □

1.2 Topology

Definition 1.13. A *metric space* is a set X endowed with a distance map $d : X \times X \to [0, \infty)$; that is, the d satisfies the following conditions for all $x, y, z \in X$:

(i) $d(x, y) = d(y, x)$

(ii) $d(x, y) = 0 \iff x = y$

(iii) $d(x, y) \leq d(x, z) + d(z, y)$.

Any norm (and therefore any absolute value) induces a *distance* on the ambient space, thus making it a Hausdorff space with the induced topology. Recall that said topology is the one where the open sets are generated by the open balls

$$\{B(x, r); r > 0, x \in X\}, \quad B(x, r) = \{y \in X; d(y, x) < r\}.$$

More than that, a generalized absolute value $|\cdot|$ also induces a Hausdorff topology on F via the similar procedure (though not necessarily a distance). Namely, the topology will be generated by

$$\{B(x, r); r > 0, x \in F\}, \quad B(x, r) = \{y \in F; |y - x| < r\}.$$

Exercise 1.1. Prove that F becomes a Hausdorff topological space with the above topology.

Definition 1.14. Two norms or two generalized absolute values are *equivalent* if they induce the same topology on the ambient space.

Proposition 1.15. *Two generalized absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field F are equivalent if and only if there exist a positive constant c such that $|a|_1 = |a|_2^c$ for all $a \in F$.*

Proof. ($\Leftarrow$) $B_{|\cdot|_2}(x, r) = \{y \in F; |y - x|_2 < r\} = \{y \in F; |y - x|_1 < r^c\} = B_{|\cdot|_1}(x, r^c)$
($\Rightarrow$) We know that $|x|_1 < 1 \iff x^n \to 0$ in the topology induced by $|\cdot|_1$. Since the two topologies are the same, it follows that

$$|x|_1 < 1 \iff |x|_2 < 1. \tag{1.1}$$

Taking inverses, we see that

$$|x|_1 > 1 \iff |x|_2 > 1. \tag{1.2}$$

Therefore we also have

$$|x|_1 = 1 \iff |x|_2 = 1. \tag{1.3}$$

Pick two nonzero elements a, b of F and set

$$x_{m,n} = a^m b^n \text{ for all } m, n \in \mathbb{Z}.$$

By plugging $x_{m,n}$ in each of (1.1), (1.2) and (1.3) and taking logarithms we see that, for any integers m, n

$$\begin{aligned} m\log|a|_1 + n\log|b|_1 > 0 &\iff m\log|a|_2 + n\log|b|_2 > 0 \\ m\log|a|_1 + n\log|b|_1 = 0 &\iff m\log|a|_2 + n\log|b|_2 = 0 \\ m\log|a|_1 + n\log|b|_1 < 0 &\iff m\log|a|_2 + n\log|b|_2 < 0 \end{aligned}$$

Therefore

$$\frac{\log|a|_1}{\log|a|_2} = \frac{\log|b|_1}{\log|b|_2} = c > 0,$$

and hence $|a|_1 = |a|_2^c$ for all $a \in F$. □

Remark 1.16. *This is in contrast to the equivalence of two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on a F-vector space V compatible with the same absolute value $|\cdot|$ on F. The two norms are equivalent if and only if there exist $m, M > 0$ such that $m\|v\|_1 \leq \|v\|_2 \leq M\|v\|_1$ for all $v \in V$.*

Proposition 1.17. (1) *Any generalized absolute value is equivalent to a generalized absolute value which satisfies property (iii) of Definition 1.8 with $C = 2$.*

(2) *A generalized absolute value satisfies property (iii) of Definition 1.8 with $C = 2$ if and only if it satisfies the triangle inequality, i.e. $|a+b| \leq |a| + |b|$ for all $a, b \in F$.*

Proof. (1) If $|\cdot|$ satisfies (*iii*) with $C \leq 2$, then it also satisfies it with $C = 2$. Otherwise, just take $|\cdot|^c$ where $c = \log_C 2$.

(2) Assume that it satisfies the triangle inequality.
Then, if $|a| \leq 1$ we have

$$|1 + a| \leq |1| + |a| \leq 1 + 1 = 2.$$

Conversely, assume that $|1 + x| \leq 2$ whenever $|x| \leq 1$. If $a = 0$ or $b = 0$, the triangle inequality is trivially satisfied. Let $a, b \in F^\times$. Then $A = \max\{|a|, |b|\} > 0$ and $|a + b| \leq 2A$. First we prove that

$$|a_1 + \ldots + a_r| \leq 2r \max\{|a_j|; 1 \leq j \leq r\} \text{ for any } a_1, \ldots, a_r \in F.$$

By induction we see that

$$\left|\sum_{j=1}^{2^s}\right| \leq 2^s \max\{|a_j|; 1 \leq j \leq 2^s\}.$$

For any $r > 0$ there exists $s > 0$ such that $2^{s-1} \leq r < 2^s$. By completing the sum with zeroes as needed, we see that

$$\left|\sum_{j=1}^{r} a_j\right| \leq 2^s \max\{|a_j|; 1 \leq j \leq r\} \leq 2r \max\{|a_j|; 1 \leq j \leq r\}$$

In particular, for any integer n we have $|n| = |1 + \cdot + 1| \leq 2n|1| = 2n$. Therefore

$$\begin{aligned} |a+b|^n &\leq \left|\sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}\right| \\ &\leq 4(n+1)\max\{\binom{n}{j}|a|^j|b|^{n-j}; 0 \leq j \leq n\} \\ &\leq 4(n+1)(|a|+|b|)^n. \end{aligned}$$

Raising to the power $\frac{1}{n}$ and taking $\lim_{n\to\infty}$ we get that indeed $|a+b| \leq |a| + |b|$.

□

Thus any generalized absolute value is equivalent to a bonafide absolute value (norm). The only reason we even introduced the notion of generalized absolute value is that we want the square of the absolute value on $\mathbb{C}$ to be part of the same class of objects as the absolute value on $\mathbb{R}$ and $\mathbb{Q}$.

1.3 Non-archimedean vs archimedean

Example 1.18. Let p be a prime number and for any nonzero integer m define $v_p(m)$ to be the highest power of p that divides m. That is, $v_p(m) \in \mathbb{Z}_{\geq 0}$ such that $p^{v_p(m)} \mid m$, but $p^{v_p(m)+1} \nmid m$. Set $v_p(0) = \infty$. The map

$$v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$$

is well defined on $\mathbb{Q}$ and

$$|x|_p = p^{-v_p(x)}$$

defines an absolute value on $\mathbb{Q}$ called the *p-adic absolute value* (with the convention $p^{-\infty} = 0$.)

Exercise 1.2. Prove that v_p is indeed a well defined map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ and that for any $x, y \in \mathbb{Q}$ we have

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x) \in \mathbb{Z}$ for any nonzero rational x;
3. $v_p(x+y) = \min\{v_p(x), v_p(y)\}$ if $v_p(x) \neq v_p(y)$
4. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

Exercise 1.3. Prove that $|\cdot|_p$ defines an absolute value and that $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x, y \in \mathbb{Q}$ with equality when $|x|_p \neq |y|_p$.

We will write $|\cdot|_\infty$ for the usual absolute value on $\mathbb{Q}$.

Definition 1.19. An absolute value $|\cdot|$ on a field F is called *non-archimedean* if it satisfies the strong triangle inequality $|a+b| \leq \max\{|a|, |b|\}$ for all $a, b \in F$ and *archimedean* otherwise. Same for norms on vector spaces.

As we have seen, $|\cdot|_p$ is non-archimedean. So is the trivial absolute value. But $|\cdot|_\infty$ is archimedean.

Remark 1.20. *We group here a few easy observations about non-archimedean absolute values.*

(1) If $|\cdot|$ is a non-archimedean absolute value on a field F then

$$|a+b| = \max\{|a|, |b|\} \text{ whenever } |a| \neq |b|. \tag{1.4}$$

(2) If $|\cdot|$ is a non-archimedean absolute value then the set

$$R = \{a \in F; |a| \leq 1\}$$

is a ring.

(3) An absolute value is non-archimedean if and only if it satisfies property (iii) of Definition 1.8 with $C = 1$.

(4) If two generalized absolute values are equivalent and one of them is non-archimedean, then so is the other.

Proof. (1) Assume $0 < |a| < |b|$. Then $|b| \leq \max\{|a+b|, |a|\}$, so $|b| \leq |a+b| \leq |b|$.

(2) If $a, b \in R$, then clearly $|ab|, |a-b| \in R$.

(3) If $|\cdot|$ is non-archimedean, and $|a| \leq 1$, then $|1+a| \leq \max\{|1|, |a|\} = 1$.
Conversely, assuem $0 < |a| \leq |b|$. Then $|ab^{-1}| \leq 1$, and therefore $|1+ab^{-1}| \leq 1$, which implies $|a+b| \leq |b|$.

(4) Assume $|\cdot|_1 \sim |\cdot|_2$ and that $|\cdot|_1$ is non-archimedean. We know that there exists $c > 0$ such that $|x|_2 = |x|_1^c$ for all $x \in F$. Assume that $|a|_2 \leq |b|_2$. This implies that $|a|_1 \leq |b|_1$ and therefore $|a+b|_1 \leq |b|_1$. But then

$$|a+b|_2 = |a+b|_1^c = |b|_1^c = |b|_2.$$

□

Lemma 1.21. *Two non-archimedean absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if the two rings they generate $R_1 = \{a \in F; |a|_1 \leq 1\}$ and $R_2 = \{a \in F; |a|_2 \leq 1\}$ coincide.*

Proof. ($\Rightarrow$) clear
($\Leftarrow$) $|a|_1 < |b|_1 \iff ab^{-1} \in R_1$ and $a^{-1}b \notin R_1$. Since $R_1 = R_2$, the two topologies coincide.

□

Lemma 1.22. *An absolute value $|\cdot|$ on a field F is non-archimdean if and only if $|n| \leq 1$ for all n in the subring generated by 1 in F.*

Proof. $(\Rightarrow)$ $|1+1+\cdots+1| \leq |1| = 1$.
$(\Leftarrow)$ Let $a \in F$ with $|a| \leq 1$. Then

$$|1+a|^n \leq \sum_{j=0}^{n} \left|\binom{n}{j}\right| |a|^j \leq n+1.$$

Taking n-th roots and then $\lim_{n\to\infty}$ we get that $|1+a| \leq 1$. □

Theorem 1.23 (Ostrowski)**.** *Every non-trivial generalized absolute value is equivalent to either the p-adic absolute value $|\cdot|_p$ for some prime p or to the usual absolute value $|\cdot|_\infty$.*

Proof. Since any generalized absolute value is equivalent to some absolute value, we can reduce to this case. Let $|\cdot|$ be some non-trivial absolute value on $\mathbb{Q}$. Fix an integer $a > 1$. Then any other nonnegative integer b can be written in base a, as

$$b = b_m a^m + \cdots + b_0, \quad 0 \leq b_j < a, \quad m \leq \log_a b = \frac{\ln b}{\ln a}.$$

Let $M = \max\{|n|; 0 < n < a\}$. Then $M \geq 1$ and $|b_j| \leq M$ for all $0 \leq j \leq m$ and therefore

$$|b| \leq M(|a|^m + \cdots + 1) \leq M(m+1)\max\{1, |a|^m\} \leq M\left(\frac{\ln b}{\ln a} + 1\right)\max\{1, |a|^{\frac{\ln b}{\ln a}}\}$$

Replacing $b = c^n$ for some $c \geq 1$ above gives

$$|c| \leq M^{\frac{1}{n}}\left(n\frac{\ln c}{\ln a} + 1\right)^{\frac{1}{n}}\max\{1, |a|^{\frac{\ln c}{\ln a}}\},$$

which, as $n \to \infty$, implies that

$$|c| \leq \max\{1, |a|^{\frac{\ln c}{\ln a}}\}. \tag{1.5}$$

Case 1: There exist $c \in \mathbb{Z}$ such that $|c| > 1$.

We can assume without loss of generality that c is a positive integer. Then any integer $a > 1$ satisfies (1.5) and therefore $|a| > 1$. Moreover, in this case (1.5) implies that

$$|c|^{\frac{1}{\ln c}} \leq |a|^{\frac{1}{\ln a}}.$$

Since the situation is completely symmetric in a and c we also have the inequality

$$|c|^{\frac{1}{\ln c}} \geq |a|^{\frac{1}{\ln a}},$$

so in reality

$$|c|^{\frac{1}{\ln c}} = |a|^{\frac{1}{\ln a}} \text{ for all integers } a, c > 1.$$

Denote by ρ this constant, which is greater than 1. Then

$$|a| = \rho^{\ln a} = e^{\ln \rho \ln a} = a^{\ln \rho} \text{ for all positive integers } a$$

and

$$|\cdot| = |\cdot|_\infty^{\ln \rho}.$$

Case 2: $|c| \leq 1$ for all $c \in \mathbb{Z}$.

Then, by Lemma 1.22, $|\cdot|$ is non-archimedean. Since $|\cdot|$ is non-trivial, there exist some positive integer with norm strictly less than 1. Let p be the smallest such positive integer. Let

$$I = \{a \in \mathbb{Z}; |a| < 1\}.$$

Then

$$a, b \in I \implies |a + b| \leq \max\{|a|, |b|\} < 1 \implies a + b \in I$$

and

$$a \in I, n \in \mathbb{Z} \implies |na| = |n||a| \leq |a| < 1 \implies na \in I.$$

Thus I is an ideal and since p is the smallest positive integer in I, we get $I = p\mathbb{Z}$. On the other hand if $a, b \in Z$ and $ab \in I$ then $|a||b| = |ab| < 1$ and either $|a| < 1$ or $|b| < 1$. Hence I is a prime ideal, which forces p to be prime. Let $\rho = |p| \in (0, 1)$. If q is a prime number and $q \neq p$, then $q \notin I$, and thus $|q| = 1$. Any integer $n > 1$ can be written as a product of primes

$$n = p^a q_1^{a_1} \dots q_r^{a_r},$$

where $a \geq 0$, $q_j \neq p$ and $a_j > 0$ for $1 \leq j \leq r$. Then $a = v_p(a)$ and

$$|n| = |p|^a |q_1|^{a_1} \dots |q_r|^{a_r} = \rho^a = \rho^{v_p(a)}.$$

Therefore $|\cdot| \sim |\cdot|_p$.

□

Remark 1.24. *The p-adic absolute value induces the p-*adic metric (distance) *and p-*adic topology *on $\mathbb{Q}$. This is very different from the Euclidean topology that we are used to. For instance* 1 *and* 1000000000001 *are as close in $|\cdot|_3$ than* 1 *and* 2.

Another different feature, that is actually common to all non-archimedean norms: Exercise 1.3 implies that any triangle has two equal sides in the p-adic metric.

An even more striking feature is the following. If $\|\cdot\|$ is a non-archimedean norm on a space V, and take any point

$$b \in B(a, r) = \{x \in V; \|x - a\| < r\}$$

then

$$B(a, r) = B(b, r).$$

Indeed, for any $x \in B(a,r)$,

$$\|x-b\| \leq \max\{\|x-a\|, \|b-a\|\} < r \implies x \in B(b,r).$$

On the other hand, for any $y \in B(b,r)$,

$$\|y-a\| \leq \max\{\|y-b\|, \|b-a\|\} < r \implies y \in B(a,r).$$

2 Completions

This construction works for any metric space and it is the same way that $\mathbb{R}$ is formally constructed from $\mathbb{Q}$. We start by recalling the following definitions.

Definition 2.1. A sequence $(x_n)_{n\geq 1}$ of points in a metric space (X,d) is *Cauchy* if for any positive real number $\epsilon > 0$ there exists a positive integer N_ϵ such that

$$d(x_n, x_m) < \epsilon \text{ for all } n, m \geq N_\epsilon.$$

Definition 2.2. A metric space (X,d) is *complete* if any Cauchy sequence is convergent, i.e. it has a limit in X, i.e. for any Cauchy sequence $(x_n)_{n\geq 1}$ there exists a point $x \in X$ such that $d(x_n, x) \to 0$ as $n \to \infty$.

The following construction allows one to "complete" a metric space (X,d), that is to construct a complete metric space $(\hat{X}, \hat{d})$ together with a natural embedding $i : (X,d) \hookrightarrow (\hat{X}, \hat{d})$ such that $\hat{d} \circ (i \times i) = d$ and $i(X)$ is dense in $\hat{X}$.

Definition 2.3. The space $(\hat{X}, \hat{d})$ is called the *completion* of (X,d).

Remark 2.4. *Such a space is necessarily unique up to isometry. In particular, $\hat{d}$ is the unique distance on $\hat{X}$ that extends d.*

And we proceed with the construction. Let S denote the set of all Cauchy sequences in X. We say that two such sequences $s_1 = (x_n)_{n\geq 1}$ and $s_2 = (y_n)_{n\geq 1}$ are equivalent ($s_1 \sim s_2$) if $d(x_n, y_n) \to 0$ as $n \to \infty$.

Clearly

- $s \sim s$ for any $s \in S$;
- $s_1 \sim s_2 \implies s_2 \sim s_1$ since the distance function is symmetric;
- $s_1 \sim s_2, s_2 \sim s_3 \implies s_1 \sim s_3$ because of the triangle inequality.

Hence $\sim$ is indeed an equivalence relation. We set $\hat{X} = S/\sim$ to be the set of equivalence classes $[s]$ of Cauchy sequences and define

$$\hat{d} : \hat{X} \times \hat{X} \to [0, \infty) \quad \hat{d}([s_1],[s_2]) = \lim_{n\to\infty} d(x_n, y_n) \text{ for } s_1 = (x_n)_{n\geq 1},\ s_2 = (y_n)_{n\geq 1}.$$

This is a well-defined function because if $s_1 = (x_n)_{n\geq 1} \sim s_1' = (x_n')_{n\geq 1}$ and $s_2 = (y_n)_{n\geq 1} \sim s_2' = (y_n')_{n\geq 1}$, then

$$d(x_n', y_n') \leq d(x_n', x_n) + d(x_n, y_n) + d(y_n, y_n') \, \forall n \implies \lim_{n\to\infty} d(x_n', y_n') \leq \lim_{n\to\infty} d(x_n, y_n).$$

Similarly we get

$$\lim_{n\to\infty} d(x_n, y_n) \leq \lim_{n\to\infty} d(x_n', y_n').$$

We now have to make sure that $\hat{d}$ is a distance. Indeed,

- $\hat{d}([s_1], [s_2]) = 0 \iff d(x_n, y_n) \to 0 \iff s_1 \sim s_2 \iff [s_1] = [s_2]$
- $\hat{d}([s_1], [s_2]) = \lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} d(y_n, x_n) = hatd([s_2], [s_1])$
- $\hat{d}([s_1], [s_2]) = \lim_{n\to\infty} d(x_n, y_n) \leq \lim_{n\to\infty} \left(d(x_n, z_n) + d(z_n, y_n)\right)$ $= \lim_{n\to\infty} d(x_n, z_n) + \lim_{n\to\infty} d(z_n, y_n) = \hat{d}([s_1], [s_3]) + \hat{d}([s_3], [s_2])$

Moreover, assume that $([s_n])_{n\geq 1}$ is a Cauchy sequence in $\hat{X}$ where $s_n = (x_{n,j})_{j\geq 1}$. We want to construct a Cauchy sequence $s = (y_j)_{j\geq 1} \in S$ such that $\hat{d}([s_n], [s]) \to 0$ as $n \to \infty$. To this end, pick a decreasing sequence of positive reals $\epsilon_j \to 0$. Since $([s_n])_{n\geq 1}$ is Cauchy, for each $j \geq 1$ there exits M_j such that

$$d(x_{j,m}, x_{j,m}) < \epsilon_j \text{ for all } n, m \geq M_j.$$

Set $y_j = x_{j,M_j} \in X$. We will show two things about the sequence $s = (y_n)_{n\geq 1}$ is Cauchy in (X, d) and that $\hat{d}([s_n], [s]) \to 0$ as $n \to \infty$.

Fix $\epsilon > 0$. There exists $k_\epsilon \geq 1$ such that

$$\epsilon_k < \frac{\epsilon}{3} \text{ for all } k \geq k_\epsilon.$$

There also exists N_ϵ such that $\hat{d}([s_n], [s_m]) = \lim_{j\to\infty} d(x_{n,j}, x_{m,j}) < \epsilon/3$ and therefore there exists some N_ϵ' such that

$$d(x_{n,j}, x_{m,j}) < \frac{\epsilon}{3} \text{ for all } j \geq N_\epsilon'.$$

Let $A_\epsilon = \max\{k_\epsilon, N_m, N_n\}$.

Let $m, n \geq A_\epsilon$. Choose $r \geq \max\{M_m, M_n, N_\epsilon'\}$. Then $d(x_{m,r}, x_{n,r}) < \epsilon/3$ and

$$\begin{aligned} d(y_m, y_n) = d(x_{m,M_m}, x_{n,M_n}) &\leq d(x_{m,M_m}, x_{m,r}) + d(x_{m,r}, x_{n,r}) + d(x_{n,r}, x_{n,M_n}) \\ &< \epsilon_m + \frac{\epsilon}{3} + \epsilon_n < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon. \end{aligned}$$

So now that we have proved that s is a Cauchy sequence, we will use this fact to show that $\hat{d}([s_n], [s]) \to 0$ as $n \to \infty$. Set $B_\epsilon = \max\{A_{\frac{\epsilon}{3}}, k_\epsilon\}$. Let $k \geq B_\epsilon$ and choose some $r \geq \max\{B_\epsilon, M_k\}$. We have

$$d(x_{k,r}, y_r) \leq d(x_{k,r}, x_{k,M_k}) + d(y_k, y_r) \leq \epsilon_k + \frac{\epsilon}{3} < \frac{2\epsilon}{3}.$$

Taking the limit as $r \to \infty$ this yields

$$\hat{d}([s_k],[s]) \leq \frac{2\epsilon}{3} < \epsilon$$

and we have proved completeness.

The original space X embeds into $\hat{X}$ via the map $i(x) = [x]$ where $[x]$ is the equivalence class of the constant sequence (x_n) with all terms $x_n = x$. Clearly this is a Cauchy sequence, $i : X \to \hat{X}$ is an injection and $\hat{d} \circ (i \times i) = d$. (Note that this implies that i is continuous.) It remains to prove that $i(X)$ is dense in $\hat{X}$. This is guaranteed, since for any $s = (x_n) \in S$ we have

$$\hat{d}([i(x_n)],[s]) = \lim_{m\to\infty} d(x_n, x_m) \text{ and } d(x_n, x_m) \to 0 \text{ as } n, m \to \infty.$$

□

We can start with a field F and an absolute value $|\cdot|$ on it. We know that this induces a metric $d(a,b) = |a-b|$ on F with respect to which F becomes a metric space. The completion of this metric space is $(\hat{F}, \hat{d})$. Identify F with its embedded image into $\hat{F}$.

Proposition 2.5. *$\hat{F}$ is a field and $|x|' = \hat{d}(x,0)$ defines an absolute value that extends $|\cdot|$. Moreover, $\hat{F}$ is unique up to isomorphism and $|\cdot|'$ is the unique absolute value that extends $|\cdot|$.*

Proof. The fact that addition and multiplication are well-defined is immediate. It is also clear that $0_{\hat{F}} = 0_F$, $1_{\hat{F}} = 1_F$ and $-[(a_n)] = [(-a_n)]$. With these operations $\hat{F}$ is a commutative ring. The only part that requires some work is to show that inverses exist. Let $[s] = [(x_n)] \in \hat{F}$ such that $s \not\sim 0$. Then $|x_n| \not\to 0$, i.e. for any $\epsilon > 0$ there exists a subsequence (x_{n_j}) of (x_n) such that $|x_{n_j}| > \epsilon$. We can assume without loss of generality that $|x_n| > \epsilon$ for all n. Then $x_n \in F^\times$ and $0 < |x_n^{-1}| < \frac{1}{\epsilon}$. Let $s' = (y_n)$ where $y_n = x_n^{-1}$. Since s is Cauchy, it follows that there exists N_ϵ such that for $m, n \geq N_\epsilon$ we have $|x_n - x_m| < \epsilon^3$. Then

$$|y_n - y_m| = \frac{|x_m - x_n|}{|x_n|\,|x_m|} < \epsilon \text{ for } m, n \geq N_\epsilon.$$

Therefore s' is Cauchy and it is the multiplicative inverse of $[s]$. □

Corollary 2.6. *Every field F with a generalized absolute value $|\cdot|$ can be embedded in a complete field $\hat{F}$ with a generalized absolute value $|\cdot|'$ extending the original one in such a way that $\hat{F}$ is the closure of F with respect to $|\cdot|'$. Further, $\hat{F}$ is unique up to isomorphism.*

Corollary 2.7. *$|\cdot|'$ is non-archimedean on $\hat{F}$ if and only if $|\cdot|$ is non-archimedean on F. In this case, the set of values taken be $|\cdot|'$ and $|\cdot|$ are the same.*

Proof. ($\Rightarrow$) trivial
($\Leftarrow$) The ring generated by 1 is the same in the two fields. Now apply Lemma 1.22.

Now we want to prove that the two absolute values have the same image in $[0, +\infty)$. Clearly the image of $|\cdot|$ is contained in the image of $|\cdot|'$. Let $x \in \hat{F}, x \neq 0$. Then there exists $a \in F$ such that

$$|x - a|' < |x|'.$$

By Remark 1.20, this can happen only if $|x|' = |a|' = |a|$.

□

Remark 2.8. *This is in sharp contrast with the archimedean case. For instance, the absolute value on $\mathbb{R}$ takes many more values than the absolute value on $\mathbb{Q}$ that it extends (e.g. $\sqrt{2}, \pi$, etc).*

Corollary 2.9. *Any embedding of F into a complete field K that preserves the absolute value can be uniquely continued to an embedding of $\hat{F}$ (that will also preserve the absolute value).*

From now on we will denote $|\cdot|$ the extension of the absolute value on F to its completion $\hat{F}$.

2.1 The field $\mathbb{Q}_p$

Fix a prime number p. Then the p-adic absolute value on $\mathbb{Q}$ defined by $\left|\frac{m}{n}\right|_p = p^{v_p(n)-v_p(m)}$ is a non-archimedean absolute value whose image consists of

$$\{0\} \cup \{p^n; n \in \mathbb{Z}\}.$$

Definition 2.10. The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$.

According to the definition, $\mathbb{Q}_p$ consists of equivalence classes of Cauchy sequences. But we can give a more concrete description as follows.

Lemma 2.11. *If $x \in \mathbb{Q}$ with $|x|_p \leq 1$, then for each $n \geq 1$ there exists an integer $a_n \in \{0, 1, \ldots, p^n - 1\}$ such that $|a_n - x|_p \leq p^{-n}$.*

Proof. Write $x = \frac{a}{b}$ such that $(a, b) = 1$. Since $|x|_p \leq 1$ we must have $p \nmid b$. So $(b, p^n) = 1$ and therefore we can find integers m, n such that $mb + np^n = 1$. Set $a_n = am$. Then

$$|x - a_n|_p = \left|\frac{a}{b} - am\right|_p = \left|\frac{a}{b}\right|_p |1 - mb|_p \leq |1 - mb|_p = |np^n|_p \leq \frac{1}{p^n}.$$

□

Theorem 2.12. *Every element of $a \in \mathbb{Q}_p$ (i.e. every equivalence class of Cauchy sequences) with $|a|_p \leq 1$ is represented by exactly one Cauchy sequence $(a_n)_{n\geq 1}$ with*

(i) $0 \leq a_n < p^n$ *for all* $n \geq 1$;

(ii) $a_n \equiv a_{n+1} \pmod{p^n}$ *for all* $n \geq 1$.

Proof. **Uniqueness** Assume $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ are two such sequence.
If they are different, then there exits $j \geq 1$ such that $a_j \neq b_j$. But since $a \leq a_j, b_j < p^j$ this means that $a_j \not\equiv b_j \,(\mathrm{mod}\ p^j)$. But for all $n \geq j$ we have $a_n \equiv a_j \,(\mathrm{mod}\ p^j)$ and $b_n \equiv b_j$ $(\mathrm{mod}\ p^j)$. This implies that $a_n \not\equiv b_n \,(\mathrm{mod}\ p^j)$, and so

$$|a_n - b_n|_p > \frac{1}{p^j} \text{ for all } n \geq j.$$

Hence $(a_n)_{n\geq 1} \not\sim (b_n)_{n\geq 1}$.

Existence Assume that $(b_n)_{n\geq 1}$ is a Cauchy sequence in $\mathbb{Q}$ with respect to the p-adic norm that is in the equivalence class $a \in \mathbb{Q}_p$.

We want to find an equivalent sequence $(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$ with the required properties. Fix $j \geq 1$. Then there exists $N_j \geq j$ such that

$$|b_i - b_r|_p < p^{-j} \text{ for all } i, r \geq N_j.$$

We can take without loss of generality the sequence $(N_j)_{j\geq 1}$ to be strictly increasing. For each $i \geq N_1$ we have for $r > i$,

$$|b_i|_p = |b_i + b_r - b_r|_p \leq \max\{|b_r|_p, |b_r - b_i|_p\} \leq \max\left\{|b_r|_p, \frac{1}{p}\right\}$$

Then letting $r \to \infty$ we have $|b_r|_p \to |a|_p$, so

$$|b_i| \leq \max\{|a|_p, p^{-1}\} \leq 1.$$

By Lemma 2.11 there exists $a_j \in \mathbb{Z}$ such that $0 \leq a_j < p^j$ such that $|b_{N_j} - a_j|_p < p^{-j}$. Then

$$|a_{j+1} - a_j|_p \leq \max\{|a_{j+1} - b_{N_{j+1}}|_p, |b_{N_{j+1}} - b_{N_j}|_p, |b_{N_j} - a_j|_p\} \leq \max\{p^{-(j+1)}, p^{-j}, p^{-j}\} = p^{-j}.$$

Therefore $(a_n)_{n\geq 1}$ is a Cauchy sequence with $0 \leq a_n < p^n$ and $a_n \equiv a_{n+1} \,(\mathrm{mod}\ p^n)$.

On the other hand, for any $j \geq 1$ and $r \geq N_j$ we have

$$|a_r - b_r|_p \leq \max\{|a_r - a_j|_p, |a_j - b_{N_j}|_p, |b_i - b_{N_j}|_p\} = \max\{p^{-j}, p^{-j}, p^{-j}\} = p^{-j}.$$

Therefore $\lim_{r\to\infty} |a_r - b_r|_p = 0$ and $(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$.

□

For an arbitrary $a \in \mathbb{Q}_p, a \neq 0$ we have $|a|_p = p^r$ for some $r \in \mathbb{Z}$. Then $a = p^{-r}a'$ and $a' \in \mathbb{Q}_p$ with $|a'|_p \leq 1$. Then a' is represented by a sequence $(a'_n)_{n\geq 1}$ with $0 \leq a'_n < p^n$, and therefore a is represented by $(a_n)_{n\geq 1}$ with $a_n = p^{-r}a'_n$. We can write all the a'_n's in base p, as

$$a'_n = b_0 + \cdots + b_{n-1}p^{n-1},$$

with $b_i \in \{0, 1, \ldots, p-1\}$. The condition $a'_n \equiv a'_{n+1} \pmod{p^{n+1}}$ means that

$$a_{n+1} = b_0 + \cdots + b_{n-1}p^{n-1} + b_n p^n$$

has the same first $(n-1)$ base p digits as a_n. Thus a' can be thought intuitively as number written in base p that extends infinitely far to the right. Our original number a is then a base p decimal number with finitely many digits "'to the right" of the decimal point, but infinitely many "to the left", i.e.

$$a = \frac{b_0}{p^r} + \frac{b_1}{p^{r-1}} + \cdots + \frac{b_{r-1}}{p} + b_r + b_{r+1}p + \ldots . \tag{2.1}$$

Note that $S_n = \sum_{j=0}^{n} b_j p^{j-r}$ is the sequence of partial sums of the series on the right hand side of (2.1). Then for any n we have

$$|a - S_n|_p = \left| \sum_{j=n+1}^{\infty} b_j p^{j-r} \right|_p \leq p^{r-n-1} \overset{n\to\infty}{\longrightarrow} 0,$$

which means that indeed a is the sum of the series (in the same sense as in $\mathbb{R}$).

Moreover, if $(c_n)_{n\neq 0} \in \mathbb{Q}_p$ is a sequence of p-adic numbers with $|c_n| \to 0$, we can form the series $\sum\limits_{n=0}^{\infty} c_n$. The sequence of partial sums

$$S_N = \sum_{n=0}^{N} c_n$$

is Cauchy because for $M > N$

$$|S_M - S_N|_p = \left| \sum_{n=N+1}^{M} c_n \right|_p \leq \max\{|c_{N+1}|_p, \ldots, |c_M|_p\} \overset{N\to\infty}{\longrightarrow} 0.$$

Thus we have proved the following result.

Proposition 2.13. *An infinite p-adic series converges if and only if its terms approach* 0.

Remark 2.14. *The uniqueness in Theorem 2.12 is something we do not have in the archimedean case. For instance,* $1 = 0.99999\ldots$ *in* $\mathbb{R}$*, i.e. terminating decimal expansions can also be represented with infinitely repeating decimals. But in* $\mathbb{Q}_p$*, if two p-adic expansions converge to the same limit in* $\mathbb{Q}_p$*, then they are the same, i.e. all their digits coincide.*

Remark 2.15. *If* $(\alpha_n)_{n\geq 1} \subset \mathbb{Q}_p$ *is convergent, that means that each p-adic digit in the sequence has to stabilize after a while. To make this precise, think of* $|a_n|_p$*. This is a convergent sequence in the set* $\{p^n; n \in \mathbb{Z}\} \cup \{0\}$*, and therefore it has a maximum. Thus there is some*

$r \in \mathbb{Z}$ such that each term of our sequence of p-adic number a_n has p-adic digit expansion of the form

$$a_n = \sum_{j \geq r} b_{nj} p^j .$$

Pushing this reasoning further, we use the fact that for any $t \geq 0$ there exists $N_t \geq 1$ such that

$$|a_m - a_n| < \frac{1}{p^t} \forall n, m \geq N_t \implies b_{mj} = b_{nj} \forall n, m \geq N_t, r \leq j \leq t.$$

This means that for any $j \geq r$ there exists $M_j \geq 1$ such that

$$b_{nj} = b_{M_j j} \text{ for all } n \geq M_j .$$

Another feature of the p-adic digit expansion is that if $a = \sum a_n p^n$, then $|a|_p = p^{-m}$ where $m = \min\{n \in \mathbb{Z}; a_n \neq 0\}$. Thus $|a|_p \leq 1$ if and only if its p-adic digit expansion contains only non-negative powers of p, i.e. a is of the form

$$a = \sum_{n=0}^{\infty} a_n p^n .$$

Definition 2.16. We define $\mathbb{Z}_p = \{a \in \mathbb{Q}_p; |a|_p \leq 1\}$ the set of *p-adic integers. We can think of $\mathbb{Z}$ as the set of* rational integers.

Since $|\cdot|_p$ is non-archimedean, we know by Remark 1.20 that $\mathbb{Z}_p$ is a subring of the field $\mathbb{Q}_p$.

Definition 2.17. We say that two p-adic numbers $a, b \in \mathbb{Q}_p$ are *congruent modulo p^n* and write $a \equiv b \pmod{p^n}$ if $|a - b|_p \leq p^{-n} \iff a - b \in p^n \mathbb{Z}_p$.

Note that if a, b happen to be rational integers, this definition agrees with the usual congruence relation in $\mathbb{Z}$.

The mechanics of adding, subtracting, multiplying and dividing p-adic numbers are very similar to the corresponding operations in $\mathbb{R}$.

Example 2.18. Here are a few computations in $\mathbb{Q}_7$.

$$\begin{array}{rr} & \ldots 263.0 \\ + & \ldots 154.0 \\ \hline & \ldots 450.0 \end{array} \qquad \begin{array}{rr} & \ldots 632.2 \\ - & \ldots 411.6 \\ \hline & \ldots 220.3 \end{array}$$

$$\begin{array}{rr} & \ldots 263 \\ \times & \ldots 154 \\ \hline & \ldots 445 \\ + & \ldots 41 \\ + & \ldots 3 \\ \hline & \ldots 455 \end{array} \qquad \begin{array}{rcr} & & \ldots 165 \\ \cline{3-3} \ldots 153 & / & \ldots 421 \\ & & \ldots 161 \\ \hline & & \ldots 23 \\ & & \ldots 53 \\ \cline{3-3} & & \ldots 4 \\ & & \ldots 4 \\ \cline{3-3} & & \ldots \end{array}$$

As usual we write $\mathbb{Z}_p^\times$ for the group of invertible elements of the ring $\mathbb{Z}_p$.

Proposition 2.19. $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p; |x|_p = 1\} = \{x \in \mathbb{Z}_p; x \not\equiv 0 \,(\mathrm{mod}\ p)\}$.

Proof. It is clear that the two sets are equal. We also have for $x \neq 0$ that $x \in \mathbb{Z}_p^\times \iff x, 1/x \in \mathbb{Z}_p$. This means that we need both $|x|_p \leq 1$ and $|1/x|_p \leq 1$. The only way for both inequalities to be satisfied is to have $|x|_p = 1$. □

Definition 2.20. The elements of $\mathbb{Z}_p^\times$ are called *p-adic units.*

Remark 2.21. *Instead of* $\{0, 1, \ldots, p-1\}$ *we could have chosen any set* $S = \{a_0, \ldots, a_{p-1}$ *of p-adic integers such that* $a_i \equiv i \,(\mathrm{mod}\ p)$ *and defined the p-adic expansion to be of the form* $\sum_{j \geq -m} c_j p^j$ *with* $c_j \in S$. *In fact, there is another choice of representatives, called* Teichmüller representatives*, that is even more natural in some ways.*

3 Algebraic equations in $\mathbb{Q}_p$

Example 3.1. We want to find $x \in \mathbb{Q}_5$ such that $x^2 = 6$. That means that we are looking for a sequence $a_0, a_1, \dots \in \{0, 1, 2, 3, 4\}$ such that

$$(\ldots a_2 a_1 a_0)^2 = (a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \ldots)^2 = 1 + 1 \cdot 5.$$

Comparing the coefficients of 5^0 on both sides, we get that

$$a_0^2 \equiv 1 \pmod 5,$$

so $a_0 = 1$ or 4. First let's take $a_0 = 1$. Then we compare the coefficients of 5^1 on both sides and see that (since nothing carries from the previous step)

$$2a_0a_1 \cdot 5 = 2a_1 \cdot 5 \equiv 1 \pmod{5^2} \implies 2a_1 \equiv 1 \pmod 5,$$

and so $a_1 = 3$. Now we carry 1 forward and have, by looking at the coefficients of 5^2, that

$$2a_0a_2 \cdot 5^2 + a_1^2 \cdot 5^2 + 1 \cdot 5^2 = 2a_2 \cdot 5^2 + 10 \cdot 5^2 \equiv 0 \pmod{5^3} \implies 2a_2 \equiv 0 \pmod 5,$$

and thus $a_2 = 0$. As we keep going, we get that

$$x = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \cdots = \ldots 4031.$$

Each coefficient $a_i, i > 0$ in the 5-adic expansion of x is uniquely determined. If we choose $a_0 = 4$, we get by the same reasoning the solution

$$y = -x = 4 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + (4 - a_4) \cdot 5^4 + (4 - a_5) \cdot 5^5 + \cdots = \ldots (4 - a_5)(4 - a_4)0414.$$

Remark 3.2. *The fact that we had two choices for* a_0 *and then, once we chose* a_0 *the other coefficients were uniquely determined merely reflects the fact that* 6 *has exactly two square roots in* $\mathbb{Q}_5$. *In fact, just like over* $\mathbb{R}, \mathbb{Q}$, *or* $\mathbb{C}$, *a nonzero element of* $\mathbb{Q}_p$ *will have* exactly two *square roots in* $\mathbb{Q}_p$ *if it has any. But not all elements have square roots, which means that* $\mathbb{Q}_p$ *in not algebraically closed.*

Example 3.3. We want to solve the equation $x^2 = 7$ in $\mathbb{Q}_5$. As before, we are looking for a sequence $a_0, a_1, \dots \in \{0, 1, 2, 3, 4\}$ such that

$$(\dots a_2 a_1 a_0)^2 = (a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \dots)^2 = 2 + 1 \cdot 5.$$

But now we see that this implies $a_0^2 \equiv 2 \pmod 5$, which is impossible to solve since 2 is a quadratic nonresidue modulo 5. Hence 7 does not have square roots in $\mathbb{Q}_5$.

In fact, the only obstacle to a number $b \in \mathbb{Z}_5$ having square roots is the fact that its last digit might not be a quadratic residue modulo 5. Once we can solve $a_0^2 \equiv b_0 \pmod 5$, the equation for finding $b_1, b_2, \dots$ are all linear and the only coefficient that appears is 2. (This means that things in $\mathbb{Q}_2$ are more pathologic when it comes to square roots!)

This method of solving algebraic equations by solving them first $\pmod p$, then successively $\pmod{p^2}$, $\pmod{p^3} \dots$ is in fact quite general. This fact is encoded in the following result, which also explains why we would have problems finding square roots via this method in $\mathbb{Q}_2$.

Theorem 3.4 (Hensel's Lemma: Version I). *Let $F(X) = c_0 + c_1 X + \dots + c_n X^n \in \mathbb{Z}_p[X]$. Its derivative is, as usual, $F'(X) = c_1 + 2c_2 X + \dots + nc_n X^{n-1}$. Let $\alpha \in \mathbb{Z}_p$ such that*

$$|F(\alpha)|_p < |F'(\alpha)|_p^2 \tag{3.1}$$

Then there exists a unique *$a \in \mathbb{Z}_p$ such that*

$$F(a) = 0 \quad \text{and} \quad |a - \alpha|_p \le \left| \frac{F(\alpha)}{F'(\alpha)} \right|_p . \tag{3.2}$$

Proof. Note that $|F'(\alpha)|_p \le 1$ since $F'(\alpha) \in \mathbb{Z}_p$. We first look at the case $|F'(\alpha)|_p = 1$. Then (3.1) becomes

$$F(\alpha) \equiv 0 \pmod p \quad \text{and} \quad F'(\alpha) \not\equiv 0 \pmod p.$$

We prove by induction that there exists a unique sequence of rational integers $a_0, a_2, \dots \in \mathbb{Z}$ such that, for all $j \ge 0$,

1. $F(a_j) \equiv 0 \pmod{p^{j+1}}$;
2. $a_{j+1} \equiv a_j \pmod{p^{j+1}}$;
3. $0 \le a_j \le p^{j+1}$;
4. $F'(a_j) \not\equiv 0 \pmod p$.

For $j = 0$: first we denote by b_0 the unique element of $\{0, 1, \dots, p-1\}$ such that $b_0 \equiv \alpha \pmod p$ and then we set $a_0 = b_0$. This means that $a_0 \equiv \alpha \pmod p$ and hence $F(a_0) \equiv F(\alpha) \pmod p \equiv 0 \pmod p$ and $F'(a_0) \equiv F'(\alpha) \pmod p \not\equiv 0 \pmod p$. The other two properties are obviously satisfied.

For $j = 1$: if $a_1 \equiv a_0 \,(\text{mod } p)$ and $0 \leq a_1 \leq p^2 - 1$, then $a_1 = b_0 + b_1 p$ for some $b_1 \in \{0, 1, \ldots, p-1\}$. We still have to deal with the first condition.

$$\begin{aligned} F(a_1) &= F(b_0 + b_1 p) = \sum_{r=0}^{n} c_r (b_0 + b_1 p)^r = \sum_{r=0}^{n} \left(c_r b_0^r + r c_r b_0^{r-1} b_1 p + \text{ terms divisible by } p^2 \right) \\ &\equiv \sum_{r=0}^{n} c_r b_0^r + \left(\sum_{r=1}^{n} r c_r b_0^{r-1} \right) b_1 p \pmod{p^2} \equiv F(b_0) + F'(b_0) b_1 p \pmod{p^2} \end{aligned}$$

On the other hand, since $b_0 \equiv a_0 \,(\text{mod } p)$, we have

$$F(b_0) \equiv F(a_0) \pmod{p} \equiv 0 \pmod{p} \implies F(b_0) \equiv cp \pmod{p^2} \text{ for a unique } c \in \{0, 1, \ldots, p-1\}$$

and

$$F'(b_0) \equiv F'(a_0) \pmod{p} \not\equiv 0 \pmod{p}.$$

Now we see that

$$F(a_1) \equiv 0 \pmod{p^2} \iff cp + F'(a_0) b_1 p \equiv 0 \pmod{p^2} \iff c + F'(a_0) b_1 \equiv 0 \pmod{p}.$$

Since $F'(a_0) \not\equiv 0 \,(\text{mod } p)$, this equation can be solved for b_1, and it has a unique solution among $0, 1, \ldots, p-1$. We get this desired $a_1 = b_0 + b_1 p$ and our construction ensures it is unique. Furthermore, $F'(a_1) \equiv F'(a_0) \,(\text{mod } p) \not\equiv 0 \,(\text{mod } p)$.

For the induction step, we assume we already found $a_1, \ldots, a_{j-1}$ and look for a_j. By the last two properties, we need $a_j = a_{j-1} + b_j p^j$ with $0 \leq b_j \leq p-1$. When we expand $F(a_{j-1} + b_j p^j)$ around a_{j-1} as before we get

$$F(a_j) = F(a_{j-1} + b_j p^j) \equiv F(a_{j-1}) + F'(a_{j-1}) b_j p^j \pmod{p^{j+1}}$$

But we know by the induction hypothesis that $F(a_{j-1}) \equiv 0 \,(\text{mod } p^j)$, hence $F(a_{j-1}) \equiv c' p^j$ (mod p^{j+1}) for a unique $c' \in \{0, 1, \ldots, p-1\}$. Using this we see that we need to solve for b_n the equation

$$c' + F'(a_{j-1}) b_j \equiv 0 \pmod{p}.$$

The induction hypothesis also implies that

$$F'(a_{j-1}) \not\equiv 0 \pmod{p},$$

hence we can indeed solve for b_j and the solution is unique in the range allowed. Thus we have uniquely constructed a_j. Moreover $a_j \equiv a_{j-1} \,(\text{mod } p)$, hence $F'(a_j) \equiv F'(a_{j-1}) \,(\text{mod } p) \not\equiv 0$ (mod p) and we proved the induction step.

Thus we have proved the existence and uniqueness of our sequence $a_1, a_2, \ldots$. We use this to prove the theorem. Namely, set

$$a = b_0 + b_1 p + b_2 p^2 + \cdots + b_j p^j + \ldots$$

and we see immediately that

$$F(a) \equiv F(a_j) \pmod{p^{j+1}} \equiv 0 \pmod{p^{j+1}} \text{ for all } j \implies F(a) = 0.$$

On the other hand, it is equally clear that

$$a \equiv b_0 \pmod{p} \equiv \alpha \pmod{p}.$$

Conversely, every $a = b_0 + b_1 p + \dots$ gives rise to a sequence $a_j = b_0 + b_1 p + \dots + b_j p^j$, $j \geq 1$, with the three properties above. The uniqueness of the sequence implies the uniqueness of a itself and the theorem is proved in the case $|F'(\alpha)|_p = 1$.

For the arbitrary M case, one can go through the argument above in identical fashion. But here it might be more enlightening to conceptualize the procedure above as the Newton approximation that we all know and love ever since we learned calculus. (As an aside, Newton approximation appears in many guises in analysis: the implicit function theorem, the fundamental theorem of ODEs, etc. . .)

The general principle is as follows. We are looking for a solution to $f(x) = 0$ where f is a given function. We start at some point $x = a_0$. If f happened to be linear (which is the ideal of calculus), then in order to find a root all we would have to do is find the intersection of the line passing through $(a, f(a))$ with the x-axis. A simple algebraic manipulation tell us that the intersection occurs at the point $a_1 = a_0 - \dfrac{f(a_0)}{f'(a_0)}$. We compute $f(a_1)$ which will typically fail to be 0. But we can try again the same method starting at the point a_1 this time and so on, until we zero in on a root. That means that we keep iterating the transformation

$$x \to x - \frac{f(x)}{f'(x)} \tag{3.3}$$

and construct a sequence $a_0, a_1, \dots, a_n, \dots$ whose limit will (usually in $\mathbb{R}$, always in the setting of the Hensel's Lemma in $\mathbb{Q}_p$) be a root of the function $f(x)$. Just how much better the approximation of a root gets at every point is encoded in Lemma 3.5 below.

So we start by setting $x_0 = \alpha$. We have

$$\frac{|F(x_0)|_p}{|F'(x_0)|_p^2} < 1 \implies \frac{F(x_0)}{F'(x_0)} \in p\mathbb{Z}_p.$$

Now we apply the transformation (3.3) to x_0 and set

$$x_1 = x_0 - \frac{F(x_0)}{F'(x_0)} \in \mathbb{Z}_p \implies |x_1 - x_0|_p < |F'(x_0)| \implies |x_1 - x_0|_p \leq \frac{1}{p}|F'(x_0)|_p.$$

The Taylor expansion of our polynomial tells us that

$$F(x_1) = F(x_0) + (x_1 - x_0)F'(x_0) + (x_1 - x_0)^2 G(x_0, x_1)$$

with $G[Y,Z] \in \mathbb{Q}_p[Y,Z]$. But even though apriori we only have $(Y-Z)^2 \mid F(Y)-F(Z)-(Y-Z)F'(Z)$ in $\mathbb{Q}_p[Y,Z]$, since both polynomials actually have coefficients in $\mathbb{Z}_p$ and $(Y-Z)^2$ is monic, it follows that the divisibility holds over $\mathbb{Z}_p$, and that means that in fact $G[Y,Z] \in \mathbb{Z}_p[Y,Z]$. Hence $G(x_0,x_1) = b \in \mathbb{Z}_p$ and $F(x_1) = (x_1-x_0)^2 b$. Therefore

$$|F(x_1)|_p \leq |x_1 - x_0|_p^2 = \frac{|F(x_0)|_p^2}{|F'(x_0)|_p^2} < |F(x_0)|_p \leq \frac{1}{p}|F(x_0)|_p. \tag{3.4}$$

Similarly, the Taylor formula for the derivative shows that

$$F'(x_1) = F'(x_0)+(x_1-x_0)c \text{ with } c \in \mathbb{Z}_p \implies |F'(x_1)-F'(x_0)|_p \leq |x_1-x_0|_p = \frac{|F(x_0)|_p}{|F'(x_0)|_p} < |F'(x_0)|_p.$$

Hence

$$|F'(x_1)|_p = \max\{|F'(x_0)|_p, |F'(x_1)-F'(x_0)|_p\} = |F'(x_0)|_p. \tag{3.5}$$

Together (3.4) and (3.5) ensure that

$$\frac{|F(x_1)|_p}{|F'(x_1)|_p^2} < \frac{1}{p} < 1.$$

We keep iterating and obtain a sequence $(x_m)_{m\geq 0} \in \mathbb{Z}_p$ with

$$|F(x_m)|_p \leq \frac{1}{p^m}|F(x_0)|_p \overset{m\to\infty}{\longrightarrow} 0,$$

$$|F'(x_m)|_p = |F'(x_0)|_p,$$

$$|x_{m+1}-x_m|_p = \frac{|F(x_m)|_p}{|F'(x_m)|_p} \leq \frac{1}{p^m}\frac{|F(x_0)|_p}{|F'(x_0)|_p} \overset{m\to\infty}{\longrightarrow} 0.$$

Thus $(x_m)_{m\geq 0}$ is Cauchy and therefore it converges to some $a \in \mathbb{Q}_p$. But

$$|a|_p = \lim_{m\to\infty} |x_m|_p \leq 1 \implies a \in \mathbb{Z}_p,$$

which, by the way, shows that $\mathbb{Z}_p$ is complete. Moreover, $F(a) = \lim F(x_m) = 0$ and $|a - x_0| < |F'(x_0)|_p$ which is exactly what we needed since $x_0 = \alpha$.

The uniqueness of the point a follows from the fact that it is a fixed point of the contraction mapping $x \to x - \frac{F(x)}{F'(x)}$ within each set $\alpha + p^M\mathbb{Z}_p$ where $|F(\alpha)/F'(\alpha)| = p^{-M}$. A fixed point of a contraction on a complete space is necessarily unique. I leave to you the proof that this is indeed a contraction mapping.

□

Lemma 3.5. *Let $F(X) \in \mathbb{Z}_p[X]$. Let $\beta \in \mathbb{Z}_p$, $n,k \in \mathbb{Z}$ such that $0 \leq 2k < n$ and*

$$F(\beta) \equiv 0 \pmod{p^n}, |F'(\beta)|_p = p^{-k}.$$

Then there exists $y \in \mathbb{Z}_p$ such that

$$F(y) \equiv 0 \pmod{p^{n+1}},\ |F'(y)|_p = p^{-k} \text{ and } y \equiv \beta \pmod{p^{n-k}}.$$

Proof. The hypothesis tells us that $F(\beta) = p^n a$ for some $a \in \mathbb{Z}_p$ and $F'(\beta) = p^k b$ for some $b \in \mathbb{Z}_p^\times$. Because we want $y \equiv \beta \pmod{p^{n-k}}$, our y is forced to have the form $y = \beta + p^{n-k}z$ with $z \in \mathbb{Z}_p$. Taylor's formula tells us that

$$F(y) = F(\beta) + p^{n-k}zF'(\beta) + p^{2n-2k}c \text{ with } c \in \mathbb{Z}_p.$$

Hence

$$F(y) = p^n(a + bz) + p^{2n-2k}c.$$

We have $2n - 2k \geq n + 1$, so in order to ensure that $F(y) \equiv 0 \pmod{p^{n+1}}$ we need to choose $z \in \mathbb{Z}_p$ such that

$$a + bz \equiv 0 \pmod{p}.$$

Since $b \in \mathbb{Z}_p^\times$, this is always possible.

We still have to evaluate $|F'(y)|_p$, and here we employ again Taylor's formula.

$$F'(y) = F'(\beta) + p^{n-k}d, \text{ with } d \in \mathbb{Z}_p.$$

But $|p^{n-k}d| \leq p^{k-n} < p^{-k} = |F'(\beta)|_p$ and so $|F'(y)|_p = p^{-k}$.

□

Theorem 3.6 (Hensel's Lemma: Version II). *Let $F(X_1, \dots, X_m) \in \mathbb{Z}_p[X_1, \dots, X_m]$. Let $\alpha \in \mathbb{Z}_p$ such that*

$$|F(\alpha)|_p < \left|\frac{\partial F}{\partial X_j}(\alpha)\right|_p^2.$$

Then there exists $a \in \mathbb{Z}_p^m$ such that

$$F(a) = 0 \quad \textit{and} \quad |a - \alpha|_p \leq |F(\alpha)|_p \left|\frac{\partial F}{\partial X_j}(\alpha)\right|_p^{-1}.$$

Proof. Reduces to the one variable case. □

Theorem 3.7 (Hensel's Lemma: Version III). *Let $F(X), g(X), h(X) \in \mathbb{Z}_p[X]$. Assume that $g(X)$ is monic, $F(X) \equiv g(X)h(X) \pmod{p}$ and $g(X), h(X)$ are coprime modulo p. Then there exist polynomials $G(X), H(X) \in \mathbb{Z}_p[X]$ such that $G(X)$ is monic,*

$$F(X) = G(X)H(X), \quad G(X) \equiv g(X) \pmod{p}, \quad H(X) \equiv h(X) \pmod{p}.$$

Note that the monic condition ensures that $\deg G(X) = \deg g(X)$.

Proof. Similar to Version I. □

Corollary 3.8. *Suppose $p \neq 2$. Let*

$$f = \sum_{i,j=1}^{n} a_{ij}X_iX_j$$

with $a_{ij} = a_{ji}$ be a quadratic form in n variables with coefficients in $\mathbb{Z}_p$ and $a \in \mathbb{Z}_p$. Assume that $\det(a_{ij})_{1\le i,j\le n} \in \mathbb{Z}_p^\times$. *Then every solution $x \not\equiv 0 \,(\text{mod } p)$ of the equation*

$$f(x) \equiv a \pmod p$$

lifts to a true solution.

Proof. Since $x \not\equiv 0 \,(\text{mod } p)$ and $\det(a_{ij})_{1\le i,j\le n} \not\equiv 0 \,(\text{mod } p)$, it follows that there exists $1 \le j \le n$ such that

$$\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \pmod p.$$

By Hensel's Lemma (Version II, Theorem 3.6) this implies that there exists $y \in \mathbb{Z}_p$ such that $f(y) = a$ and $y \equiv x \,(\text{mod } p)$. □

Corollary 3.9. *Let*

$$f = \sum_{i,j=1}^{n} a_{ij} X_i X_j$$

with $a_{ij} = a_{ji}$ be a quadratic form in n variables with coefficients in $\mathbb{Z}_2$ and let $a \in \mathbb{Z}_2$. Let $x \not\equiv 0 \,(\text{mod } 2)$ be a solution of

$$f(x) \equiv a \pmod 8.$$

Then we can lift x to a true solution provided $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \,(\text{mod } 4)$ for some j. The condition holds if $\det(a_{ij})_{1\le i,j\le n} \in \mathbb{Z}_2^\times$.

Proof. Let $g(X) = f(X) - a$. Then

$$\frac{\partial g}{\partial X_j}(x) = \sum_{i=1}^{n} 2a_{ij}x_i \equiv 0 \pmod 2.$$

On the other hand, we know that

$$\frac{\partial g}{\partial X_j}(x) \not\equiv 0 \pmod 4,$$

and therefore

$$\left|\frac{\partial g}{\partial X_j}(x)\right|_2 = \frac{1}{2} \implies |g(x)|_2 \le \frac{1}{8} < \frac{1}{4} = \left|\frac{\partial g}{\partial X_j}(x)\right|_2^2.$$

Thus we can apply Hensel's Lemma (Version II, Theorem 3.6) again and deduce that there exists $y \in \mathbb{Z}_2$ such that $f(y) = a$ and $y \equiv x \,(\text{mod } 4)$.

All that is left to prove is that the condition that $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \,(\text{mod } 4)$ for some j holds when $\det(a_{ij})_{1\le i,j\le n} \in \mathbb{Z}_2^\times$. But the condition is equivalent to

$$\sum_{i=1}^{n} a_{ij}x_i \not\equiv 0 \pmod 2 \text{ for some } j$$

which is immediate if $\det(a_{ij})_{1\le i,j\le n} \not\equiv 0 \,(\text{mod } 2)$ and $x \not\equiv 0 \,(\text{mod } 2)$.

□

3.1 Square roots in $\mathbb{Q}_p$

Proposition 3.10. *Suppose $p \neq 2$ and let $x \in \mathbb{Q}_p^\times$. We know that x can be written uniquely as $x = p^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Then x is a square if and only if n is even and u (mod p) is a quadratic residue modulo p.*

Proof. First if $x = y^2$ for some $y \in \mathbb{Q}_p^\times$, then we write $y = p^m v$ with $m \in \mathbb{Z}$ and $v \in \mathbb{Z}_p^\times$. It follows that $n = 2m$ and $u = v^2$. Conversely, assume that there exists $v \in \{1, \dots, p-1\}$ such that $u \equiv v^2 \pmod{p}$. Then we apply Corollary 3.8 to the quadratic form $f = X^2$ and see that there exist $y \in \mathbb{Z}_p$ such that $y^2 = u$ and $y \equiv v \pmod{p}$. In particular, $y \in \mathbb{Z}_p^\times$. If in addition n is even, it follows that x is a square. □

Pick $\alpha \in \{1, \dots, p-1\}$ (or in $\mathbb{Z}_p^\times$) that is a quadratic nonresidue modulo p. Choose any $x \in \mathbb{Q}_p^\times$. Again, $x = p^n u, n \in \mathbb{Z}, u \in \mathbb{Z}_p^\times$.

If n is even and u is a quadratic residue modulo p, then $x \in \left(\mathbb{Q}_p^\times\right)^2$.

If n is even and u is a quadratic nonresidue modulo p, then $x\alpha{-}1$ is a square, so $x \in \alpha\left(\mathbb{Q}_p^\times\right)^2$.

If n is odd, then similarly $x \in p\left(\mathbb{Q}_p^\times\right)^2$ or $x \in p\alpha\left(\mathbb{Q}_p^\times\right)^2$.

The product of each two of the elements $1, \alpha, p, p\alpha$ is not a square, hence they are the distinct elements of $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2$. In particular, we have the following result.

Corollary 3.11. $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *for $p > 2$.*

Proposition 3.12. *An element $x \in \mathbb{Q}_2^\times$ can be written uniquely as $x = 2^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_2^\times$. Then x is a square if and only if n is even and $u \equiv 1 \pmod{8}$.*

Proof. If $x = y^2$ for some $y = 2^m v$, with $m \in \mathbb{Z}$ and $v \in \mathbb{Z}_2^\times$, then $n = 2m$ and $u \equiv v^2 \pmod{8}$. But $v \equiv 1 + 2a_1 \pmod{4}$ with $a_1 = 0, 1$. Hence $u \equiv 1 + 4a_1 + 4a_1^2 \pmod{16} \equiv 1 \pmod{8}$. Conversely, if $u \equiv 1 \pmod{8}$, it means that we can apply Corollary 3.9 to the quadratic form $f = X^2$ and u itself. It follows that u is a square. If in addition n is even, then x is also a square. □

Corollary 3.13. $\mathbb{Q}_2^\times / \left(\mathbb{Q}_2^\times\right)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *with representatives* $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Proof. Similar to the case $p > 2$. Instead of quadratic nonresidues, one has to consider elements of the form $1 + 2a_1 + 4a_2 \pmod{8}$ with $a_1, a_2 = 0, 1$. □

3.2 The structure of units

Definition 3.14. For every $n > 0$ set $U_n = 1 + p^n \mathbb{Z}_p$.

Note that

$$\mathbb{Z}_p^\times \supset U_1 \supset U_2 \supset \dots$$

form a fundamental system of neighborhoods of 1 in $\mathbb{Q}_p$. They are all open subgroups of $\mathbb{Z}_p^\times$ with respect to multiplication.

Lemma 3.15. *The canonical map $\mathbb{Z}_p \to \mathbb{F}_p, x \to x\,(\text{mod } p)$ is a surjective ring homomorphism. The induced group homomorphism $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ is surjective and has kernel U_1. Thus $\mathbb{Z}_p^\times/U_1 \simeq \mathbb{F}_p^\times$.*

Proof. Clear. □

Lemma 3.16. *For $n \geq 1$, the map $1 + p^n x \mapsto x\,(\text{mod } p)$ induces an isomorphism*

$$U_n/U_{n+1} \xrightarrow{\sim} \mathbb{F}_p.$$

Proof. Since $U_n = 1 + p^n\mathbb{Z}_p$ every element $u \in U_n$ can be written uniquely at $u = 1 + p^n x$ with $x \in \mathbb{Z}_p$. Thus the map $f : U_n \to \mathbb{F}_p$ given by $f(1 + p^n x) = x\,(\text{mod } p)$ is well-defined. Moreover, for $x, y \in \mathbb{Z}_p$ we have

$$(1 + p^n x)(1 + p^n y) = 1 + p^n(x + y) + p^{2n}xy \equiv 1 + p^n(x + y) \pmod{p^{n+1}}$$

which implies that

$$f((1 + p^n x)(1 + p^n y)) \equiv x + y \pmod{p} = f(1 + p^n x) + f(1 + p^n y),$$

so f is a group homomorphism. It is clear that f is surjective. On the other hand,

$$1 + p^n x \in \ker f \iff x \equiv 0 \pmod{p} \iff 1 + p^n x \in 1 + p^{n+1}\mathbb{Z}_p = U_{n+1}.$$

□

Proposition 3.17.

$$\mathbb{Z}_p^\times = U_1 \times V,$$

where $V = \{x \in \mathbb{Z}_p^\times; x^{p-1} = 1\}$ is the unique subgroup of $\mathbb{Z}_p^\times$ isomorphic to $\mathbb{F}_p^\times$.

Proof. We will prove the existence of V by applying Hensel's Lemma to $F(X) = X^{p-1} - 1$. Then $F'(X) = (p-1)X^{p-2}$. For each $1 \leq j \leq p-1$ we have $F(j) \equiv 0\,(\text{mod } p)$ and $F'(j) \not\equiv 0$ $(\text{mod } p)$. Hence there exists a unique $a_j \in \mathbb{Z}_p$ such that $a_j \equiv j\,(\text{mod } p)$ and $F(a_j) = 0$. In particular, $a_j \not\equiv 0\,(\text{mod } p)$ and so $a_j \in \mathbb{Z}_p^\times$ for all $1 \leq j \leq p-1$. Then $V = \{a_1, \ldots, a_{p-1}\}$ and it has exactly $p - 1$ elements. By the way, $a_1 = 1$ and a_j are precisely the nonzero Teichmüller representatives.

Also, $a_j a_n \equiv jn\,(\text{mod } p)$ and $a_j a_n$ is a root of $F(X)$. By uniqueness, $a_j a_n = a_{jn}$ for any $1 \leq j, n \leq p-1$, so the map $g : j \mapsto a_j$ induces a group isomorphism $\mathbb{F}_p^\times \simeq V \subset \mathbb{Z}_p^\times$.

For uniqueness, assume V' is a subgroup of $\mathbb{Z}_p^\times$ isomorphic to $\mathbb{F}_p^\times$. Then for any $v \in V'$ we would have $v^{p-1} = 1$. Hence $V' \subseteq V$ and since they both have exactly $p - 1$ elements, $V' = V$.

Let $h : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ $h(x) = x\,(\text{mod } p)$. Since $j \to a_j \to a_j\,(\text{mod } p)$ is the identity map on $\mathbb{F}_p^\times$, we have $h \circ g = \mathrm{Id}_{\mathbb{F}_p}$. Moreover, $\ker h = U_1$ and $h \circ g = \mathrm{Id}_{\mathbb{F}_p}$.

Now $U_1 \cap V = \{a_j; a_j \equiv 1\,(\text{mod } p)\} = \{a_1\} = \{1\}$ and for any $x \in \mathbb{Z}_p^\times$ there exists some j such that $x \equiv a_j\,(\text{mod } p)$. Then $xa_j^{-1} \equiv 1\,(\text{mod } p)$, so $x = a_j y$ for some $y \in U_1$. Hence $\mathbb{Z}_p^\times = U_1 \times V$.

□

Corollary 3.18. *The field $\mathbb{Q}_p$ contains $p-1$ distinct $(p-1)$st roots of unity.*

Lemma 3.19. *Assume $n \geq 1$ and $p \neq 2$ or $n \geq 2$ and $p = 2$. Let $x \in U_n \setminus U_{n+1}$. Then $x^p \in U_{n+1} \setminus U_{n+2}$.*

Proof. See Homework 4. □

Proposition 3.20. *(i) If $p \neq 2$, then $1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$.*

(ii) $1 + 2\mathbb{Z}_2 = \{\pm 1\} \times (1 + 2^2\mathbb{Z}_2)$ and $1 + 2^2\mathbb{Z}_2 \simeq \mathbb{Z}_2$.

Proof. See Homework 4. □

Theorem 3.21.

$$\mathbb{Q}_p^\times \simeq \begin{cases} \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \neq 2 \\ \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & \text{if } p = 2. \end{cases}$$

Proof. Let $x \in \mathbb{Q}_p^\times$. Then x can be written uniquely as $x = p^n u$ with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Thus

$$\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p^\times.$$

On the other hand, Proposition 3.17 proves that $\mathbb{Z}_p^\times = V \times U_1$, where V is cyclic of order $p-1$ and the structure of U_1 is given by Proposition 3.20. □

4 Fractional ideals

Let R be an integral domain (i.e. commutative ring with $1 \neq 0$ and no zero divisors) and K its field of fractions.

Definition 4.1. For any R-submodules I, I_1, I_2 of K we define

$$(I_1 : I_2) = \{x \in K; xI_2 \subset I_2\}.$$

Two notable particular cases of this construction are

$$I^{-1} = (R : I) = \{x \in K; xI \subset R\}$$

and

$$R(I) = (I : I) = \{x \in K; xI \subset I\}.$$

Remark 4.2. *If I, I_1, I_2 of K are R-submodules of K, then $I_1 + I_2$, $I_1 \cap I_2$, $I_1 I_2$, $(I_1 : I_2)$, I^{-1} and $R(I)$ are also R-submodules of K.*

Definition 4.3. A nonzero R-submodule I of K is a *fractional ideal* of R if there exists $a \in R \setminus \{0\}$ such that $aI \subset R$.

Remark 4.4. *In this case aI is a nonzero* integral ideal *(i.e. ordinary ideal) of R.*

Definition 4.5. A fractional ideal of the form xR for some $x \in K$ is called *principal.*

Example 4.6. Take $R = \mathbb{Z}$. Then $K = \mathbb{Q}$.

1. $\frac{1}{2}\mathbb{Z}$, $\frac{3}{2}\mathbb{Z}$ are fractional ideals.

2. $\left\{\frac{m}{p^n}; m, n \in \mathbb{Z}\right\}$ is a $\mathbb{Z}$-submodule of $\mathbb{Q}$, but not a fractional ideal.

Remark 4.7. *All fractional ideals of $\mathbb{Z}$ are principal. In general, all fractional ideals of a principal ideal domain are principal.*

Proposition 4.8. *If I, I_1, I_2 are fractional ideals of R, then $I_1 + I_2$, $I_1 \cap I_2$, I_1I_2, $(I_1 : I_2)$, I^{-1} and $R(I)$ are also fractional ideals.*

Proof. We know that they are all R-submodules of K. The sum $I_1 + I_2$ and the product I_1I_2 are nonzero since I_1 and I_2 are themselves nonzero. On the other hand, if $I_1 \cap I_2 = 0$, then $I_1 \oplus I_2 \subset K$ and that would create divisors of zero in the field K. Hence $I_1 \cap I_2 \neq 0$.

We also know that there exists $a_1, a_2 \in R \setminus \{0\}$ such that $a_1I_1, a_2I_2 \subset R$. Then $a_1a_2 \neq 0$ and $a_1a_2(I_1 + I_2), a_1a_2(I_1I_2), a_1(I_1 \cap I_2) \subset R$.

Pick $b \in I_1, b \neq 0$. Then $a_1b \in I_1 \cap R$. Let $c = a_1a_2b \in (I_1 : I_2)$, since $cx = a_1b(a_2x) \in (a_1b)R \subset (I_1 \cap R)R \subset I_1$ for all $x \in I_2$. And clearly $c \neq 0$, so $(I_1 : I_2) \neq 0$.

Pick $d \in I_2, d \neq 0$. Then, for any $y \in (I_1 : I_2)$ we have $a_1a_2dy \in a_1I_1 \subset R$. Since $a_1a_2d \neq 0, a_1a_2d \in R$ it follows that $(I_1 : I_2)$ is a fractional ideal.

The last two are particular cases of $(I_1 : I_2)$.

□

Proposition 4.9. *(i) Any non-zero finitely generated R-submodule I of K is a fractional ideal.*

(ii) If R is noetherian, the converse holds: every fractional ideal is a finitely generated R-submodule of K.

Proof. (i) If $I = Rx_1 + \ldots Rx_n$ with $x_1, \ldots, x_n \in K$, then we can write $x_j = \frac{a_j}{b}$ with $b, a_1, \ldots, a_n \in R$. Thus $bI \subset R$.

(ii) If I is a fractional ideal, then there exists $a \in K^\times$ such that $aI = J$ is an ideal of R. Since R is noetherian, J is finitely generated. And so is $I = a^{-1}J$.

□

Definition 4.10. An R-submodule M of K is an *invertible ideal* if there exists an R-submodule N of K such that $MN = R$.

In this case, the submodule N is unique and $N = (R : M) = M^{-1}$. To see this, note that

$$N \subseteq (R : M) = (R : M)R = (R : M)MN \subseteq RN \subseteq N.$$

It follows that there exist $x_1, \dots, x_n \in M$ and $y_1, \dots, y_n \in M^{-1}$ such that

$$x_1y_1 + \cdots + x_ny_n = 1.$$

Hence any $x \in M$ can be written as

$$x = a_1x_1 + \cdots + a_nx_n,$$

where $a_j = xy_j \in MM^{-1} = R$. Thus M is finitely generated, and therefore a fractional ideal.

Example 4.11. Every principal fractional ideal (a) is invertible, its inverse being the principal fractional ideal (a^{-1}).

Remark 4.12. *The invertible ideals form a group with respect to multiplication, whose identity element is $R = (1)$. The principal fractional ideals form a subgroup of the group of invertible ideals.*

Lemma 4.13. *If M, N are R-submodules of K and N is finitely generated, then $S^{-1}(M : N) = (S^{-1}M : S^{-1}N)$ for any multiplicative system $S \subset R \setminus \{0\}$.*

Proof. Note that the field of fractions of $S^{-1}R$ is also K. Assume $x \in S^{-1}(M : N)$. Then $x = \frac{a}{s}$ with $a \in (M : N)$ and $s \in S$. Any element of $S^{-1}N$ is of the form $\frac{b}{t}$ with $b \in N$ and $t \in S$. Then

$$x\frac{b}{t} = \frac{ab}{st}$$

and $st \in S$, while $ab \in (M : N)N \subset M$, so

$$x\frac{b}{t} \in S^{-1}M.$$

Thus $x \in (S^{-1}M : S^{-1}N)$. For the other inclusion we need to use the fact that N is finitely generated, i.e. $N = Rx_1 + \cdots + Rx_n$. Then

$$(M : N) = \bigcap_{j=1}^{n} \{a \in K; ax_j \in M\} = \bigcap_{j=1}^{n} (M : Rx_j).$$

Let $y \in (S^{-1}M : S^{-1}N)$. Pick $s \in S$. We know that, for each $1 \leq j \leq n$, we have

$$y\frac{x_j}{s} = \frac{m_j}{t_j}$$

for some $m_j \in M, t_j \in S$. Let $t = t_1 \dots t_n \in S$ and $s_j = t_1 \dots t_{j-1}st_{j+1} \dots t_n \in S \subset R$. Then $ytx_j = m_js_j \in M$ so $yt \in (M : Rx_j)$ for all j.

□

Definition 4.14. If $\mathfrak{p}$ is a prime ideal of R, we denote its *localization at* $\mathfrak{p}$ by

$$R_{\mathfrak{p}} = \{\frac{a}{b}; a, b \in R, b \notin \mathfrak{p}\} = S^{-1}R,$$

where $S = R \setminus \mathfrak{p}$.

Theorem 4.15. *Invertibility is a local property. That is, for every fractional ideal I the following are equivalent:*

(i) I is invertible;

(ii) I is finitely generated and for each prime ideal $\mathfrak{p}$ of R, $I_\mathfrak{p}$ is an invertible ideal of $R_\mathfrak{p}$;

(iii) I is finitely generated and for each maximal ideal $\mathfrak{m}$ of R, $I_\mathfrak{m}$ is an invertible ideal of $R_\mathfrak{m}$.

Proof. We begin by observing that $S^{-1}(M : N) = (S^{-1}M : S^{-1}N)$ for any multiplicative system $S \subset R \setminus \{0\}$ and any R-submodules M, N of K.

($i \implies ii$) Since I is invertible, it is finitely generated. Hence $R_\mathfrak{p} = (II^{-1})_\mathfrak{p} = I_\mathfrak{p}(R : I)_\mathfrak{p} = I_\mathfrak{p}(R_\mathfrak{p} : I_\mathfrak{p})$ by the previous Lemma.

($ii \implies iii$) Every maximal ideal is prime.

($iii \implies i$) Denote by $J = II^{-1} = I(R : I)$. This is an integral ideal. Then for each maximal ideal $\mathfrak{m}$ we have $J_\mathfrak{m} = I_\mathfrak{m}(R_\mathfrak{m} : I_\mathfrak{m}) = R_\mathfrak{m}$, since $I_\mathfrak{m}$ is invertible. Therefore

$$1 = \frac{a}{b}, a \in J, b \notin \mathfrak{m} \implies a = b \in J \setminus \mathfrak{m}.$$

Thus $J \not\subseteq \mathfrak{m}$ for any maximal ideal $\mathfrak{m}$, so $J = R$.

□

5 Discrete valuation rings

Definition 5.1. A *discrete valuation* on a field K is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that

(i) v defines a surjective group homomorphism $v : K^\times \to \mathbb{Z}$;

(ii) $v(0) = \infty$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$ (with the usual conventions for ∞).

Example 5.2. The p-adic valuation v_p on $\mathbb{Q}$ is a discrete valuation.

Example 5.3. Let $K = F(X)$ the rational function field in one variable over a field F. Fix $f \in F[X]$ an irreducible polynomial. Then v_f can be defined just as the p-adic valuation, and it gives a discrete valuation on K.

Example 5.4. Again, $K = F(X)$ the rational function field over a field F. Then $v_\infty\left(\frac{f}{g}\right) = \deg g - \deg f$ defines a discrete valuation on $F(X)$. Here we use the usual convention that $\deg 0 = -\infty$.

Remark 5.5. *If v is a discrete valuation on the field K, and $0 < \rho < 1$, then $|x|_v = \rho^{v(x)}$ is a non-archimedean absolute value on K. Conversely, if $|\cdot|$ is non-archimedean absolute value on K, it induces a discrete valuation $v(x) = -c \log |x|$, where the constant c is chosen such that condition (i) is satisfied. Equivalent non-archimedean absolute values correspond to the same discrete valuation v, only the ρ changes. That is, a discrete valuation v corresponds to an equivalence class of absolute values. In particular, v induces a (well-defined) topology on K.*

The connection with the theory of absolute values means that discrete valuations have the following properties.

Proposition 5.6. *Let v be a discrete valuation on the field K.*

(i) $v(x+y) = \min\{v(x), v(y)\}$ *whenever* $v(x) \neq v(y)$.

(ii) The set $R_v = \{x \in K; v(x) \geq 0\}$ *is an integral domain with field of fractions K and* $R_v^\times = \{x \in K; v(x) = 0\}$.

(iii) The set $\mathfrak{p}_v = \{x \in K; v(x) > 0\}$ *is the unique maximal ideal of* R_v.

Proof. (i) See Remark 1.20.

(ii) The same Remark 1.20 tells us that R_v is a ring and $R_v^\times = \{x \in K; v(x) = 0\}$. Since $R_v \subset K$ and $0, 1 \in R_v$ it follows that R_v is indeed an integral domain. On the other hand, $v : K^\times \to \mathbb{Z}$ is surjective, so there exists $\pi \in K^\times$ with $v(\pi) = 1$. Then $\pi \in R_v$ and for every element of $x \in K^\times$ we have $v(x) = nv(\pi)$ for some $n \in \mathbb{Z}$. Hence $v(x\pi^{-n}) = 0$, and therefore $x = \pi^n u$ for some $u \in R_v^\times$. In particular, x is an element of the fraction fields of R_v.

(iii) We know that $R_v \setminus \mathfrak{p}_v = R_v^\times$, so we only need to prove that $\mathfrak{p}_v$ is an ideal.

To see this consider $x, y \in \mathfrak{p}_v, a \in R_v$. Then $v(x) > 0, v(y) > 0$ and $v(a) \geq 0$. Hence

$$v(x+y) \geq \min\{v(x), v(y)\} > 0 \implies x + y \in \mathfrak{p}_v$$

and

$$v(ax) = v(a) + v(x) \geq v(x) > 0 \implies ax \in \mathfrak{p}_v.$$

□

Definition 5.7. The ring R_v is called the *valuation ring* of the discrete valuation v and $\mathfrak{p}_v$ is called the *valuation ideal* of v. The field $R_v/\mathfrak{p}_v$ is called the *residue field* of v

Example 5.8. The valuation ring for v_p on $\mathbb{Q}$ is $\mathbb{Z}_{(p)}$. The valuation ideal is $p\mathbb{Z}_{(p)}$ and the residue field is $\mathbb{Z}/p\mathbb{Z}$.

Example 5.9. Let $K = F(X)$ the rational function field in one variable over a field F. Fix $f \in F[X]$ an irreducible polynomial. The valuation ring of v_f is $F[X]_{(f)}$.

Example 5.10. Again, $K = F(X)$ the rational function field over a field F. The valuation ring of v_∞ is consists of rational functions with the property that the degree of the denominator is at least the degree of the numerator. The residue field is F itself. Note that the residue field does *not* have to be finite.

Example 5.11. The p-adic valuation v_p extends naturally from $\mathbb{Q}$ to $\mathbb{Q}_p$. It remains a discrete valuations on $\mathbb{Q}_p$ with valuation ring $\mathbb{Z}_p$. The residue field is $\mathbb{Z}/p\mathbb{Z}$.

Proposition 5.12. *A discrete valuation v on a field K extends uniquely to a discrete valuation on the completion $\hat{K}$ of K with respect to the induced topology.*

Proof. We know that the associated absolute value extends uniquely up to isomorphism to $\hat{K}$ and with the same set of values. But v corresponds uniquely to the whole equivalence class of absolute values, so it extends uniquely. □

Definition 5.13. For any non-empty subset $S \subset K$ we denote by $v(S) = \inf\{v(x); x \in S\}$.

Example 5.14. $v(\{0\}) = \infty, v(R_v) = 0, v(K) = -\infty$.

Note that a priori $v(S) \in \mathbb{Z} \cup \{\pm\infty\}$. But if we consider a fractional ideal I of R_v, then we know that $I \neq 0$, so $v(I) < \infty$. On the other hand, there exists $a \in R_v, a \neq 0$ such that $aI \subset R_v$. Then $v(aI) \geq 0$, so $v(a) + v(I) \geq 0$. Thus $v(I) \geq -v(a) > -\infty$. In short,

$$v(I) = \min\{v(x); x \in I\} \in \mathbb{Z}.$$

Let $\pi \in K^\times$ such that $v(\pi) = 1$. We have seen in the course of the proof of Proposition 5.6 that every element $a \in K^\times$ can be uniquely written as

$$a = \pi^n b \text{ with } b \in R_v^\times, n = v(a) \in \mathbb{Z}.$$

For a fractional ideal I of R_v there exists an element $c \in I$ such that $v(I) = v(c)$. But $c = \pi^n b$ where $b \in R_v^\times$ and $n = v(c) = v(I)$.
Claim $I = \{x \in K; v(x) \geq v(I)\} = (\pi^n) = \pi^n R_v$ where $n = v(I)$.

Proof. Since $\pi^n = cb^{-1} \in (c) \subset I$, it follows that $(\pi^n) \subset I$. On the other hand, if $x \in I$, then $v(x) \geq n = v(\pi^n)$, so $x\pi^{-n} \in R_v$. Thus $x \in (\pi^n)$. Hence $I = (\pi^n)$. Moreover this last argument holds for any element $y \in K$ with $v(y) \geq n = v(I)$, which means that each such y is contained in I. □

In particular, this implies that $\mathfrak{p}_v = (\pi)$ and that any fractional ideal I is of the form $I = \mathfrak{p}_v^{v(I)}$. Note also that $v(\pi^{-1}) = -1$, so $\pi^{-1} \notin R_v$.

These considerations imply that $\mathfrak{p}_v$ is the unique non-zero prime ideal of R_v, and fractional ideals of R_v are powers of $\mathfrak{p}_v$, and therefore principal. This makes them also invertible, and it follows that the fractional ideals of R_v form a free abelian group with one generator, i.e. isomorphic to $\mathbb{Z}$.

Definition 5.15. A *discrete valuation ring (dvr)* is a principal ideal domain with exactly one non-zero prime ideal.

Proposition 5.16. *The valuation ring R of a discrete valuation v on a field K is a discrete valuation ring. Conversely, if R is a discrete valuation ring R with field of fractions K, then there exists a unique discrete valuation v on K with valuation ring equal to R.*

Proof. We have already proved the first part. For the converse, let $\mathfrak{p} = \pi R$ be the unique non-zero prime ideal of R. In particular, up to multiplication by units, π is the unique prime element of R. But R is a unique factorization domain, so every element $x \in R, x \neq 0$ has a unique representation as

$$x = \pi^n a, n \in \mathbb{Z}_{\geq 0}, a \in R^\times.$$

Thus every element $\alpha = \frac{x}{y} \in K^\times$ has a unique representation

$$\alpha = \pi^n a, n \in \mathbb{Z}, a \in R^\times.$$

The map $v(\alpha) = n$ defines a discrete valuation on K with valuation ring $R_v = R$. The uniqueness of v follows from the uniqueness of π. □

Definition 5.17. Let $A \subseteq B$ be commutative rings with $1 \neq 0$. An element $b \in B$ is *integral over* A if it is the root of a monic polynomial with coefficients in A. The ring A is called *integrally closed in* B if every element of B that is integral over A is contained in A. If every element of B is integral over A we say that the ring B is *integral over* A.

Example 5.18. $\mathbb{Z} \subset \mathbb{R}$ and $\sqrt{2}$ is integral over $\mathbb{Z}$ but $1/2$ is not.

Definition 5.19. An integral domain is *integrally closed* if it is integrally closed inside its field of fractions.

Example 5.20. The ring $\mathbb{Z}$ is integrally closed. Any unique factorization domain is integrally closed.

Lemma 5.21. *Let A be a subring of a commutative ring B. Then for an element $x \in B$ the following are equivalent:*

(i) *x is integral over A;*

(ii) *$A[x]$ is a finitely generated A-module;*

(iii) *$A[x]$ is contained in a subring C of B such that C is a finitely generated A-module.*

Proof. $(i \implies ii)$ We know that x satisfies some equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_0, \ldots, a_{n-1} \in A$. Then $A[x]$ is generated by $1, x, \ldots, x^{n-1}$.

$(ii \implies iii)$ Take $C = A[x]$.

$(iii \implies i)$ $x \in C = Ax_1 + \cdots + Ax_n$ with $x_1, \ldots, x_n \in B$.

Then, for each $1 \leq i \leq n$, $xx_i \in C$, so

$$xx_i = \sum_{j=1}^{n} a_{ij}x_j, \text{ for some } a_{ij} \in A.$$

Then

$$M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

where $M = (\delta_{ij}x - a_{ij})_{i,j}$. Multiply by the adjoint of M and we obtain that $(\det M)C = 0$. But $1 \in C$, so $\det M = 0$. When we expand this determinant, we obtain a monic polynomial over A which has a zero at x.

□

Lemma 5.22. *Let v be a discrete valuation on the field K. Assume that $x_1, \ldots x_n \in K$ have the property that $v(x_j) > v(x_1)$ for $2 \leq j \leq n$. Then*

$$v(x_1 + \cdots + x_n) = v(x_1).$$

Proof. $v(x_2 + \cdots + x_n) \geq \min\{v(x_2), \ldots, v(x_n)\} > v(x_1)$ and the conclusion follows. □

Proposition 5.23. *An integral domain R is a discrete valuation ring if and only if it is noetherian, integrally closed and it has exactly one non-zero prime ideal.*

Proof. **($\implies$)** A dvr is by definition a PID that has only one non-zero prime ideal.
So we only have to show that it is integrally closed. Let K be the field of fractions of R and v be the unique discrete valuation on K associated to R. Let $x \in K^\times$. If x is integral over R, it satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

with $a_0, \ldots, a_{n-1} \in R = R_v$. Thus $v(a_j) \geq 0$. Assume that $v(x) < 0$. Then $v(x^n) < v(x^j) \leq v(a_jx^j)$ for $0 \leq j \leq n-1$. By Lemma 5.22,$v(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = v(x^n) \in \mathbb{Z}$. But on the other hand $v(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = v(0) = \infty$, and we have a contradiction. Thus $v(x) \geq 0$, so $x \in R_v = R$.

($\Longleftarrow$) We need to prove that R is a principal ideal domain.

We are going to show that its unique non-zero prime ideal $\mathfrak{p}$ is principal and that every nonzero element $x \in R$ has a unique representation $x = a^n u, n \in \mathbb{Z}_{\geq 0}, u \in R^\times$, where a is a generator of $\mathfrak{p}$. This fact immediately implies that R is a dvr.

Claim 1: $R(I) = R$ for all fractional ideals I of R.
It is always the case that $R(I) \supset R$. On the other hand, $R(I)$ is a fractional ideal of a noetherian ring. By Proposition 4.9, it is therefore a finitely generated R-module. And since $R[x]$ is an R-submodule and R is noetherian, it follows that $R[x]$ is in turn a finitely generated R-module. Thus x is integral over R. But R is integrally closed, and so $x \in R$.

Claim 2: $\mathfrak{p}^{-1} \supsetneq R$.
Again we will use the fact that R is noetherian. Define

$$\mathscr{S} = \{I \subset R; I \neq 0, I \text{ ideal of } R, I^{-1} \neq R\}.$$

First we show that $\mathscr{S}$ is non-empty. Pick $b \in \mathfrak{p}, b \neq 0$. Then $b \in R \setminus R^\times$, so $b^{-1} \notin R$. Thus $(bR)^{-1} = b^{-1}R \neq R$ and $bR \in \mathscr{S}$.
Since R is noetherian, there exists a maximal element J of $\mathscr{S}$. In particular $J \neq 0$. We will show that J is a prime ideal, and thus $J = \mathfrak{p}$, which will imply that $\mathfrak{p} \in \mathscr{S}$ and therefore our claim.
Let $x, y \in R$ such that $xy \in J$, but $x \notin J$. We want to show that $y \in J$. Set $I_1 = xR + J$ and $I_2 = yR + J$. These are both nonzero integral ideal of R and since $J \subsetneq I_1$ it follows that $I_1 \notin \mathscr{S}$. Thus $I_1^{-1} = R$. Since $J^{-1} \neq R$, there exists an element $z \in J^{-1} \setminus R$. Then

$$yzI_1 = z(xy)R + zyJ \subset R \implies yz \in I_1^{-1} = R.$$

We now look at

$$zI_2 = zyR + zJ \subset R.$$

It follows that $z \in I_2^{-1}$. We already know that $z \notin R$ and therefore $I_2 \in \mathscr{S}$. Since J is maximal in $\mathscr{S}$ we must have $I_2 = J$ and so $y \in J$.

Claim 3: $\mathfrak{p}\mathfrak{p}^{-1} = R$.
As is the case with every fractional ideal we have $\mathfrak{p}\mathfrak{p}^{-1} \subset R$. Thus

$$R \supset \mathfrak{p}\mathfrak{p}^{-1} \supset \mathfrak{p}R = \mathfrak{p}.$$

Therefore $\mathfrak{p}\mathfrak{p}^{-1} = R$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. But in the latter case we would have $\mathfrak{p}^{-1} \subset R(\mathfrak{p})$ and by Claim 1, $R(\mathfrak{p}) = R$. This contradicts Claim 2.
Claim 4: $\bigcap \mathfrak{p}^n = 0$.
We have

$$R \subsetneq \mathfrak{p}^{-1} \subset R\left(\bigcap \mathfrak{p}^n\right).$$

If $\bigcap \mathfrak{p}^n \neq 0$, the last term above would be equal to R (contradiction).

Now Claim 4 implies that there exists an element $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then

$$a\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = R.$$

On the other hand, if $a\mathfrak{p}^{-1} \not\subset \mathfrak{p}$, since $a \notin \mathfrak{p}^2$. This forces the ideal $a\mathfrak{p}^{-1}$ to be the whole ring R, and so $\mathfrak{p} = aR$.

Since $\bigcap \mathfrak{p}^n = 0$, it follows that every element $x \in R$ has a unique representation as

$$x = a^n u, n \in \mathbb{Z}_{\geq 0}, u \in R^\times.$$

□

Let R be a dvr with non-zero prime ideal $\mathfrak{p}$. Denote by K the fraction field of R, v the discrete valuation on K associated to R and $k = k_v = R/\mathfrak{p}$ its residue field. Then we know that the fractional ideals of R are

$$\cdots \supset \mathfrak{p}^{-1} \supset R \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots$$

and

$$\bigcap_n \mathfrak{p}^n = 0.$$

First we look into the structure of the additive group of K. We know that

$$K = \bigcup_{n \in \mathbb{Z}} \mathfrak{p}^n$$

which is a union of closed and open subgroups of $(K, +)$.

Proposition 5.24. *$\mathfrak{p}^n/\mathfrak{p}^{n+1} \simeq k$ as k-vector spaces.*

Proof. The multiplication by π^n from $R \to \mathfrak{p}^n$ induces such an isomorphism. □

The structure of the multiplicative group $K^\times$ is similar to what we have already seen in the case of $\mathbb{Q}_p$. Denote by $U_n = 1 + \mathfrak{p}^n = 1 + \pi^n R$, for $n \geq 1$ and by $u = R^\times$. Then

$$K^\times \supset R^\times \supset U_1 \supset U_2 \supset \cdots \supset U_n \supset \ldots$$

Moreover

$$\bigcap_n U_n = \{1\}.$$

The discrete valuation v induces a short exact sequence of abelian groups

$$0 \to U \to K^\times \xrightarrow{v} \mathbb{Z} \to 0.$$

There are two topologies that we could put on U : the induced topology from $K^\times$ via this short exact sequence or the subgroup topology induced by U_n's (i.e. we declare that the xU_n, $n \geq 1$, form a neighborhood basis for $x \in U$.) But these two topologies coincide and U_n are open subgroups.

Proposition 5.25. *(i) The canonical projection $R \to k = R/\mathfrak{p}$ induces a (canonical) isomorphism $U/U_1 \simeq k^\times$.*

(ii) For any $n \geq 1$, the map $u \mapsto u - 1$ induces an isomorphism $U_n/U_{n+1} \simeq \mathfrak{p}^n/\mathfrak{p}^{n+1} \simeq k$.

Proof. (i) Let $f : R \to k$ be the canonical projection. Then

$$f(a) \neq 0 \iff a \notin p \iff a \in U$$

and $f(a) = 1 \iff a \in 1 + \mathfrak{p} = U_1$.

(ii) Clearly for every $u \in U_n$ we have $u - 1 \in \mathfrak{p}^n$. Moreover, if $u_1, u_2 \in U_n$ we have

$$(u_1u_2 - 1) - (u_1 - 1) - (u_2 - 1) = (u_1 - 1)(u_2 - 1) \in \mathfrak{p}^{2n} \subset \mathfrak{p}^{n+1},$$

so the map $g : U_n \to \mathfrak{p}^n/\mathfrak{p}^{n+1}, g(u) = u - 1$ is a group homomorphism. Since $U_n = 1 + \mathfrak{p}^n$ it follows that g is surjective. On the other hand,

$$\ker g = \{u \in U_n; u - 1 \in \mathfrak{p}^{n+1}\} = U_{n+1}.$$

□

Proposition 5.26. *(i) If the* char $k = p > 0$ *then $U_n^p \subset U_{n+1}$ for all $n \geq 1$.*

(ii) If K is complete and m is a positive integers such that char $k \nmid m$*, then the map $u \mapsto u^m$ induced an automorphism on U_n for all $n \geq 1$.*

Proof. (i) It is a direct consequence of the fact that $U_n/U_{n+1} \simeq (k, +)$ and $pk = 0$.

(ii) Fix $n \geq 1$. Define $f : U_n \to U_n, f(u) = u^m$. This is clearly a group homomorphism. For every $j \geq n$ we have the following commutative diagram

$$\begin{tikzcd}
U_j/U_{j+1} \arrow[r, "f_j"] \arrow[d, phantom, "\wr"] & U_j/U_{j+1} \arrow[d, phantom, "\wr"] \\
k \arrow[r, "g"] & k
\end{tikzcd}$$

where $f_j(xU_{j+1}) = x^mU_{j+1}$ and $g(y) = my$. Since g is an automorphism of $(k, +)$, it follows that f is an automorphism of $U_j/U/_{j+1}$. Let $u \in \ker f$. If $u \neq 1$, then there exists $j \geq n$ such that $u \in U_j \setminus U_{j+1}$. But then $f_j(u) = u^m = 1$ and since f_j is injective we get that $u \in U_{j+1}$ (contradiction). Hence $u = 1$.

Let $u \in U_n$. Since f_n is surjective, it follows that there exist elements $u_0 \in U_n, w_1 \in U_{n+1}$ such that $u = u_0^m w_1$. Using the fact that f_{n+1} is surjective we find $u_1 \in U_{n+1}, w_2 \in U_{n+2}$ such that $w_1 = u_1^m w_2$. We continue in this manner and obtain two sequences $u_j, w_j \in U_{n+j}$ such that $w_j = u_j^m w_{j+1}$. Therefore

$$u = (u_0u_1 \ldots u_j)^m w_{j+1} \text{ for all } j \geq 0.$$

Since $w_j \in U_{n+j}$ and these subgroups form a neighborhood basis of 1 it follows that $w_j \to 1$. On the other hand if we set $x_j = u_0 u_1 \dots u_j, j \geq 0$, we have $x_{j+1} \equiv x_j \pmod{\mathfrak{p}^{n+j+1}}$. Hence $(x_j)_j$ is a Cauchy sequence U_n. But U_n is a closed subset of the complete fields K, and therefore complete itself. It follows that there exist $x \in U_n$ such that $u_0 u_1 \dots u_j \to x$. But then

$$u = x^n = f(x).$$

□

6 Dedekind domains

Throughout this section R will be an integral domain and K its quotient field. We know that for any prime ideal $\mathfrak{p}$ of R the local ring $R_{\mathfrak{p}}$ has maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

Lemma 6.1. $\mathfrak{p} = \mathfrak{p}R_{\mathfrak{p}} \cap R$.

Proof. Clearly $\mathfrak{p}$ is contained both in R and in $\mathfrak{p}R_{\mathfrak{p}}$. The other inclusion is also straightforward. If $x \in R \setminus \mathfrak{p}$ then $x^{-1} \in R_{\mathfrak{p}}$, so $x \notin \mathfrak{p}R_{\mathfrak{p}}$. □

Lemma 6.2. *Let J be an ideal of the local ring $R_{\mathfrak{p}}$. Then $J = (J \cap R)R_{\mathfrak{p}}$. In particular, every ideal of $R_{\mathfrak{p}}$ is of the form $IR_{\mathfrak{p}}$, where I is an ideal of R.*

Proof. First, $J \cap R \subset J$, so $(J \cap R)R_{\mathfrak{p}} \subset JR_{\mathfrak{p}} = J$. On the other hand, if $x \in J$ then $x = \frac{a}{b}$ for some $a, b \in R, b \notin \mathfrak{p}$. Then $a = bx \in J \cap R$ and hence $x = \frac{a}{b} \in (J \cap R)R_{\mathfrak{p}}$.

□

Proposition 6.3. *If R is an integral domain the following statements are equivalent.*

(i) R is noetherian, integrally closed and its non-zero prime ideals are maximal.

(ii) R is noetherian and $R_{\mathfrak{p}}$ is a discrete valuation ring for every non-zero prime ideal $\mathfrak{p}$.

(iii) All fractional ideals of R are invertible.

Definition 6.4. An integral domain that satisfies the conditions above is called a *Dedekind domain.*

Example 6.5. $\mathbb{Z}$ is a Dedekind domain.
Any dvr is a Dedekind domain.

Proof. $(i \implies ii)$ Fix $\mathfrak{p} \neq 0$ a prime ideal of R.
We will use Proposition 5.23 to show that $R_{\mathfrak{p}}$ is a dvr. We need to show that $R_{\mathfrak{p}}$ is noetherian, integrally closed and it has only one nonzero prime ideal.
Lemma 6.2 tells us that the ideals of $R_{\mathfrak{p}}$ are of the form $IR_{\mathfrak{p}}$ with I ideal of R. Since R is noetherian, I is generated by some elements $x_1, \dots x_n$ (as an R-module). But then the same

$x_1, \ldots x_n$ generate $IR_\mathfrak{p}$ as an $R_\mathfrak{p}$-module. So $R_\mathfrak{p}$ is noetherian.

Let $x \in K$ an integral element over $R_\mathfrak{p}$. Thus there exist elements $a_0, \ldots, a_{n-1}, b \in R$ with $b \notin \mathfrak{p}$ such that

$$x^n + \frac{a_{n-1}}{b} x^{n-1} + \cdots + \frac{a_0}{b} = 0.$$

It follows that bx is integral over R, and so $bx \in R$. Hence $x \in R_\mathfrak{p}$ and we showed that $R_\mathfrak{p}$ is integrally closed.

Let J be a nonzero prime ideal of $R_\mathfrak{p}$. Then $J \cap R$ is a prime ideal of R and Lemma 6.2 implies that $J \cap R \neq 0$. On the other hand, since J is a nontrivial ideal of $R_\mathfrak{p}$ we have $J \subset \mathfrak{p}R_\mathfrak{p}$. Therefore $J \cap \mathfrak{p} \subset \mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p}$. And now Lemma 6.2 implies that $J = (J \cap R)R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$.

$(ii \implies iii)$ Let I be a fractional ideal of R.

Since R is noetherian, we know from Proposition 4.9 that I is a finitely generated R-module. On the other hand, $I_\mathfrak{p}$ is a fractional ideal of the dvr $R_\mathfrak{p}$ and as such principal and therefore invertible. By Theorem 4.15, I is invertible.

$(iii \implies i)$ Let I be a fractional ideal of R. Since I is invertible (as an R-submodule of K),

we know from Section 4 that I is finitely generated. Therefore R is noetherian.

Take $x \in K$ an integral element over R. Then the *ring* $A = R[x]$ is a finitely-generated R-module (Lemma 5.21) and therefore a fractional ideal of R (Proposition 4.9). Then

$$A = AR = A(AA^{-1}) = (AA)A^{-1} = AA^{-1} = R.$$

Therefore R is integrally closed.

Let $\mathfrak{p}$ be a nonzero prime ideal of R. Denote by $\mathfrak{m}$ the maximal ideal containing $\mathfrak{p}$. We need to show that $\mathfrak{p} = \mathfrak{m}$. We know that $\mathfrak{p}\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = R$ is an ideal of R and we have $(\mathfrak{p}\mathfrak{m}^{-1})\mathfrak{m} = \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that $\mathfrak{p}\mathfrak{m}^{-1} \subset \mathfrak{p}$ or $\mathfrak{m} \subset \mathfrak{p}$. In the latter case we are done. In the former, we have $\mathfrak{m}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = R$, which is a contradiction.

□

For the rest of this section we will denote by R a Dedekind domain and by K its quotient field. Then any prime ideal $\mathfrak{p}$ of R induces a unique discrete valuation $v_\mathfrak{p}$ on K with valuation ring $R_\mathfrak{p}$.

Proposition 6.6. *Let $|\cdot|$ be a generalized absolute value on K such that $|R| \leq 1$. Then $|x| = \rho^{v_\mathfrak{p}(x)}$ for some prime ideal $\mathfrak{p}$ of R and some real number $0 < \rho < 1$.*

Proof. Since $|R| \leq 1$ it follows from Lemma 1.22 that $|\cdot|$ is nonarchimedean. Then $\{x \in R; |x| < 1\}$ is a prime ideal of R that we denote by $\mathfrak{p}$. (Indeed, $|xy| < 1 \implies |x| < 1$ or $|y| < 1$.) But $R_\mathfrak{p}$ is a dvr, and our result follows from Proposition 5.16. □

Recall that for a subset $S \subset K$ we defined $v_{\mathfrak{p}}(S) = \inf\{v_{\mathfrak{p}}(s); s \in S\}$ and showed that in the case of a fractional ideal I we have

$$v_{\mathfrak{p}}(I) = \min\{v_{\mathfrak{p}}(x); x \in I\} \in \mathbb{Z}.$$

Proposition 6.7. *The fractional ideals of a Dedekind domain R form a free abelian group $\mathscr{I}(R)$ generated by the nonzero prime ideals of R. The representation of a fractional ideal I in terms of these generators is given by*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}.$$

Moreover, locally

$$IR_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^{v_{\mathfrak{p}}(I)}.$$

Proof. Since R is a Dedekind domain, all its fractional ideals are invertible. Remark 4.12 shows that $\mathscr{I}(R)$ is an abelian group. Let J be a nonzero integral ideal of R. If $J \neq R$, there exists a maximal (and therefore nonzero prime) ideal $\mathfrak{p}_1$ of R such that $J \subset \mathfrak{p}_1 \subset R$. But then

$$J \subset J\mathfrak{p}_1^{-1} \subset R$$

are both integral ideals. If $J\mathfrak{p}_1^{-1} = R$, then $J = \mathfrak{p}_1$ can be written as product of prime ideals. If not, then there exists $\mathfrak{p}_2$ nonzero prime ideal such that $J\mathfrak{p}_1^{-1} \subset \mathfrak{p}_2$ and therefore

$$J \subset I\mathfrak{p}_1^{-1} \subset I\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \subset R.$$

We keep going. By the ascending chain condition, the process has to stop at some point, which means that there exist nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ such that $J\mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1} = R$, and so

$$J = \mathfrak{p}_1 \dots \mathfrak{p}_n.$$

If I is a fractional ideal, then there exists $a \in R, a \neq 0$ such that $aI = J$ is a nonzero integral ideal of R. But we know that both J and aR can be factored as product of prime ideals. It follows that I can be written as a finite product of positive and negative powers of prime ideals. Therefore $\mathscr{I}(R)$ is generated by the nonzero prime ideals of R.

Fix a nonzero prime ideal $\mathfrak{p}$. Denote by $f_{\mathfrak{p}} : \mathscr{I}(R) \to \mathscr{I}(R_{\mathfrak{p}})$ the natural localization map. For any two integral ideals I, J of R we have

$$f_{\mathfrak{p}}(I)f_{\mathfrak{p}}(J) = (IR_{\mathfrak{p}})(JR_{\mathfrak{p}}) = (IJ)R_{\mathfrak{p}} = f_{\mathfrak{p}}(IJ),$$

so $f_{\mathfrak{p}}$ is a group homomorphism. By Lemma 6.2, this homomorphism is surjective and it acts injectively on the subgroup of $\mathscr{I}(R)$ generated by $\mathfrak{p}$ since $f_{\mathfrak{p}}(\mathfrak{p}^n) = \mathfrak{p}^n R_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^n$. On the other hand, for any $\mathfrak{q} \neq \mathfrak{p}$ we have $\mathfrak{q}R_{\mathfrak{p}} = R_{\mathfrak{p}}$, so $\mathfrak{q} \in \ker f_{\mathfrak{p}}$.

Assume that $\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r} = R$. Then, for each $1 \leq j \leq r$, we have $R_{\mathfrak{p}_j} = f_{\mathfrak{p}_j}(\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}) = f_{\mathfrak{p}_j}(\mathfrak{p}_j^{n_j}) \implies n_j = 0$. Hence the nonzero prime ideals form a free generating set for $\mathscr{I}(R)$.

On the other hand if $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ then $f_{\mathfrak{p}}(I) = IR_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^{n_{\mathfrak{p}}}$. Then

$$n_{\mathfrak{p}} = v_{\mathfrak{p}}(IR_{\mathfrak{p}}) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(R) = v_{\mathfrak{p}}(I).$$

□

Corollary 6.8. *If $a \in K^\times$, then $v_\mathfrak{p}(a) = 0$ for almost all nonzero prime ideals $\mathfrak{p}$.*

Proof. Clear. □

Corollary 6.9. *The discrete valuation $v_\mathfrak{p}$ behaves on fractional ideals as follows:*

$$v_\mathfrak{p}(I_1 I_2) = v_\mathfrak{p}(I_1) + v_\mathfrak{p}(I_2), \quad v_\mathfrak{p}(I_1 + I_2) = \min\{v_\mathfrak{p}(I_1), v_\mathfrak{p}(I_2)\},$$

$$v_\mathfrak{p}(I_1 \cap I_2) = \max\{v_\mathfrak{p}(I_1), v_\mathfrak{p}(I_2)\}, \quad v_\mathfrak{p}(I^{-1}) = -v_\mathfrak{p}(I).$$

Corollary 6.10. *The maps $f_\mathfrak{p}$ induce an isomorphism $\mathscr{I}(R) \simeq \bigoplus_\mathfrak{p} \mathscr{I}(R_\mathfrak{p})$.*

Remark 6.11. *Proposition 5.12 implies that $\mathscr{I}(R_\mathfrak{p}) = \mathscr{I}(\hat{R}_\mathfrak{p})$ where $\hat{R}_\mathfrak{p}$ denotes the valuation ring of the completion of K at $v_\mathfrak{p}$ (i.e. with respect to the topology induced by $v_\mathfrak{p}$). Moreover, this ideal group is isomorphic to $\mathbb{Z}$ since all the fractional ideals of a dvr are integer powers of the prime ideal.*

Corollary 6.12. $\mathscr{I}(R) \simeq \bigoplus_\mathfrak{p} \mathscr{I}(\hat{R}_\mathfrak{p}) = \bigoplus_\mathfrak{p} \mathbb{Z}$.

Fröhlich uses the notation $\coprod_\mathfrak{p}$ because what we have here is the coproduct in the category of abelian groups. However, the coproduct in the category of abelian groups (or modules over a commutative ring in general) is different from the coproduct in the category of sets. One is the direct sum, the other is the disjoint union. The convention in category theory is to use the notation coming from the category of sets.

Proposition 6.13. *If R is a Dedekind domain, then R is a unique factorization domain if and only if R is a principal ideal domain.*

Proof. Assume R has unique factorization. Since every nonzero ideal factors as a product of prime ideals, it is enough to show that the prime ideals are principal. Let $\mathfrak{p}$ be a nonzero prime ideal of R and $x \in \mathfrak{p}, x \neq 0$. Then x is not a unit, and thus it factors as a product $x = p_1 \dots p_n$ of irreducible elements. We have $p_1 \dots p_n \in \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal. Therefore there exists $1 \leq j \leq n$ such that $p_j \in \mathfrak{p}$. But (p_j) is a nonzero prime ideal, and since R is a Dedekind domain, that makes (p_j) maximal. It follows that $\mathfrak{p} = (p_j)$ is principal.

□

7 Modules and bilinear forms

In this section we introduce notions that will come in handy later in the discussion about ideal norms, differents and discriminants for extensions of Dedekind domains. First, a few words about notation. For the moment, R will be an integral domain and K its quotient field. Let V be a finite dimensional K-vector space. Then V has a natural structure of A-module.

Definition 7.1. We say that an R-submodule $M \subset V$ *spans* V if it contains a K-basis of V.

If $\mathfrak{p}$ is some nonzero prime ideal of R and M is an R-module, we denote by $M_{\mathfrak{p}} = MR_{\mathfrak{p}}$ the $A_{\mathfrak{p}}$-module generated by M.

Lemma 7.2. *For any integral domain R and any R-module M, we have $\bigcap\limits_{\mathfrak{p}} M_{\mathfrak{p}} = M$ where $\mathfrak{p}$ runs through a family of nonzero prime ideals of R that contains the maximal ideals.*

Proof. We have

$$M \subset \bigcap_{\mathfrak{p}} M_{\mathfrak{p}} \subset \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$$

where $\mathfrak{m}$ runs over the maximal ideals of R.
Conversely, let $x \in \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$. Set

$$J(x) = \{a \in R; ax \in M\}.$$

This is an integral ideal of R. For every maximal ideal $\mathfrak{m}$ there exist $b \in M$ and $y \in R \setminus \mathfrak{m}$ such that $x = \frac{b}{y}$. Thus $yx = b \in M$, so $y \in J(x)$. It follows that $J(x) \not\subset \mathfrak{m}$.
Therefore $J(x) = R$ and so $x \in M$. □

Lemma 7.3. *Given two finitely generated R-submodules M and N that span the finitely generated K-vector space V, there is a nonzero element $a \in R$ such that $aM \subset N$.*

Proof. Let $v_1, \dots, v_n$ a K-basis for V that is contained in N and $w_1, \dots, w_n$ a K-basis for V that is contained in M. Then

$$w_i = \sum_{j=1}^{n} x_{ij} v_j \text{ for all } 1 \leq i \leq n, \text{ with } x_{ij} \in K.$$

Take a to be the common denominator for all the x_{ij}. □

Now we go back to the case when R is a Dedekind domain. For the rest of this section, V will denote a finitely generated K-vector space and L, M, N will be finitely generated R-submodules of V that span V. We will use the letter T to denote an arbitrary R-submodule of V.

Lemma 7.4. *For almost all $\mathfrak{p}$, we have $M_{\mathfrak{p}} = N_{\mathfrak{p}}$.*

Proof. By the previous lemma, there exist nonzero elements $a, b \in K$ such that $aM \subset N \subset bM$. Then $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ whenever $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(b) = 0$, since in that case a, b are both units in $R_{\mathfrak{p}}$. There are only finitely many $\mathfrak{p}$'s for which the relationship does not hold (by Corollary 6.8). □

If M and N happen to be free R-modules (this is too good to be true, but it helps us understand the situation), they are isomorphic since they both have rank $n = \dim_K V$. There exists a linear transformation $\ell \in GL(V)$ such that $\ell(M) = N$. This ℓ can be constructed by considering B_1, B_2 two K-basis of V such that $B_1 \subset M$ and $B_2 \subset N$ and taking the K-linear automorphism of V that send B_1 to B_2. The determinant of ℓ depends, up to multiplication by a unit in R, only on M and N. (Here we used the fact that any automorphism of a free R-module of rank n is given by a matrix in $\mathrm{GL}(n, R)$. Using different basis contained in M or N amounts to multiplication by such a matrix.) Hence the fractional ideal $\det(\ell)R$ depends only on M and N. We will denote it by

$$[M : N] = \det(\ell)R. \tag{7.1}$$

Now, if we only know that M and N are finitely generated and they span V, we cannot make the same reasoning. However, in this case $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are free $R_\mathfrak{p}$-modules of rank $n = \dim_K V$ because of the following lemma.

Definition 7.5. Let X be a module over a ring A. An element $x \in X$ is called *torsion* if there exists $a \in A, a \neq 0$ such that $ax = 0$. The set of such elements X_{tors} is called the *torsion submodule* of X. We say that X is *torsion-free* if $X_{\text{tors}} = 0$.

Lemma 7.6. *If X is a finitely generated torsion-free module over a discrete valuation ring A, then X is a free A-module.*

The result actually holds for principal ideal domains, but the proof is particularly simple in the case of a dvr.

Proof. Fix π a generator of the maximal ideal of A. Let $x_1, \dots, x_n$ be a set of generators for X over A. If they are linearly independent over A, we are done. If not, there exist elements $a_1, \dots, a_n$ not all zero, such that

$$a_1x_1 + \cdots + a_nx_n = 0. \tag{7.2}$$

Since A is a dvr, each $a_j = u_j\pi^{m_j}$ with $u_j \in A^\times$ and $m_j \geq 0$. We can assume without loss of generality that $a_1 \neq 0$ and $m_1 \leq m_j$ for all $1 \leq j \leq n$. Thus (7.2) becomes

$$u_1\pi^{m_1}(x_1 + b_2x_2 + \cdots + b_nx_n) = 0$$

for some $b_2, \dots, b_n \in A$. Since X is torsion-free it follows that

$$x_1 + b_2x_2 + \cdots + b_nx_n = 0,$$

so $x_2, \dots, x_n$ generate X. We keep going until we are left with a linearly independent subset of generators, i.e. a basis. □

In our setup, M and N are torsion-free since they are contained in a vector space and the same holds for $M_\mathfrak{p}$ and $N_\mathfrak{p}$. Thus the previous considerations give us a fractional ideal $[M_\mathfrak{p} : N_\mathfrak{p}]$ of $R_\mathfrak{p}$. Note that whenever $M_\mathfrak{p} = N_\mathfrak{p}$ (and this happens for almost all $\mathfrak{p}$ according to Lemma 7.4) we get $[M_\mathfrak{p} : N_\mathfrak{p}] = R_\mathfrak{p}$ since we can take ℓ to be the identity map. Thus Corollary 6.10 tells us that there exists a unique fractional ideal of R,

$$[M : N] = [M : N]_R,$$

such that for all nonzero prime ideals $\mathfrak{p}$ of R

$$[M : N]R_\mathfrak{p} = [M_\mathfrak{p} : N_\mathfrak{p}]. \tag{7.3}$$

Note that in the case that M and N are actually free, the ideal given by (7.3) is the same as the one in (7.1). Moreover, in the case of the Dedekind domain $R = \mathbb{Z}$, we recover the notion of subgroup index, viewed as an ideal of $\mathbb{Z}$. This last statement is immediate in case the dimension of V happens to be 1. But for abelian groups of higher rank, one needs to do linear algebra over $\mathbb{Z}$, which amounts to going through the proof of the structure theorem of abelian groups, but only in the torsion-free case.

Definition 7.7. The fractional ideal $[M : N]$ is called the *module index* of N in M.

Proposition 7.8. *If L, M, N are finitely generated R-modules that span V, then*

(i) $[M : N][N : L] = [M : L]$;

(ii) $[M : M] = R$;

(iii) $M \supset N \implies [M : N]$ *is an integral ideal;*

(iv) $M \supset N$ *and* $[M : N] = R \implies M = N$.

Proof. All four statement hold over $R_\mathfrak{p}$ for every $\mathfrak{p}$ nonzero prime ideal. The first one amounts to the fact that the determinant of the composition of two linear maps is the product of the determinants. The rest are even easier. Since they hold locally, the first three statements hold globally by definition. For the last one, we have $M_\mathfrak{p} = N_\mathfrak{p}$ for all $\mathfrak{p}$. Lemma 7.2 implies $M = N$.

□

Proposition 7.9. *If $\ell \in \mathrm{GL}(V)$, then $[\ell(M) : \ell(N)] = [M : N]$.*

Proof. Let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $[M_\mathfrak{p} : N_\mathfrak{p}] = \det(\ell_1)R_\mathfrak{p}$ where $\ell_1 \in \mathrm{GL}(V)$ such that $\ell_1(M_\mathfrak{p}) = N_\mathfrak{p}$. Then $\ell\ell_1\ell^{-1}(\ell(M_\mathfrak{p})) = \ell(N_\mathfrak{p})$ and $\ell\ell_1\ell^{-1} \in \mathrm{GL}(V)$. So $[\ell(M_\mathfrak{p}) : \ell(N_\mathfrak{p})] = \det(\ell\ell_1\ell^{-1})R_\mathfrak{p} = \det(\ell_1)R_\mathfrak{p} = [M_\mathfrak{p} : N_\mathfrak{p}]$. It remains to observe that $\ell(M)_\mathfrak{p} = \ell(M)R_\mathfrak{p} = \ell(M_\mathfrak{p})$. □

Definition 7.10. Let $B(\cdot,\cdot)$ be a nondegenerate symmetric K-bilinear form on V. The *dual module with respect to* R of an R-submodule T of V is $D(T) = D_R(T) = \{x \in V; B(x, T) \subset R\}$.

This is an R-submodule of V as well. The following results give a few properties of the dual module.

Lemma 7.11. *If M is free R-module with basis $u_1, \ldots, u_n$ that spans V, then $D(M)$ is the free R-module spanned by the dual basis $v_1, \ldots, v_n$ of V and $D(D(M)) = M$.*

Proof. This is an immediate consequence of the fact that $B(u_i, v_j) = \delta_{ij}$. □

For simplicity, we will write $D = D_R$ and $D_{\mathfrak{p}} = D_{R_{\mathfrak{p}}}$ for the rest of the section.

Proposition 7.12. *If M, N are finitely generated modules that span V, then*

(i) *$D(M)$ is a finitely generated R-module and it spans V;*

(ii) *$D(M)_{\mathfrak{p}} = D_{\mathfrak{p}}(M_{\mathfrak{p}})$;*

(iii) *$D(M) = \bigcap_{\mathfrak{p}} D_{\mathfrak{p}}(M_{\mathfrak{p}})$;*

(iv) *$D(D(M)) = M$;*

(v) *$[D(M) : D(N)] = [N : M]$.*

Proof. *(i)* M contains a free R-module N (given by the basis of V) that spans V. By Lemma 7.3, there exists another free R-module $L = bN \supset M, b \in K^\times$ that also spans V. Thus we have $L \supset M \supset N$, which implies $D(L) \subset D(M) \subset D(N)$. By Lemma 7.11 both $D(N)$ and $D(L)$ are free and span V. This proves (i).

(ii) Let $x_1, \ldots, x_n$ be a set of generators of M.

($\supset$) Suppose $v \in D_{\mathfrak{p}}(M_{\mathfrak{p}})$. Then $B(v, x_i) \in R_{\mathfrak{p}}$ for all i.

Thus $B(v, x_i) = \frac{a_i}{b}$ for some $a_i, b \in R, b \notin \mathfrak{p}$. Then $v \in b^{-1}D(M) \subset D(M)_{\mathfrak{p}}$. Therefore $D_{\mathfrak{p}}(M_{\mathfrak{p}}) \subset D(M)_{\mathfrak{p}}$.

($\subset$) $B(D_R(M_{\mathfrak{p}}), M_{\mathfrak{p}}) \subset B(D_R(M), M)R_{\mathfrak{p}} \subset R_{\mathfrak{p}}$.

(iii) Follows from (ii) and Lemma 7.2.

(iv) Follows from (ii) and Lemma 7.11.

(v) Because of (ii) it is enough to prove this for free modules M, N.

Take $u_1, \ldots u_n$ an R-basis for M and $\ell \in GL(V)$ such that $\ell(M) = N$. Then $\ell(u_1), \ldots, \ell(u_n)$ is an R-basis of N. Let $v_1, \ldots, v_n$ be the dual basis to $u_1, \ldots, u_n$. In this case, the dual basis of $\ell(u_1), \ldots, \ell(u_n)$ is given by $\ell^*(v_1), \ldots, \ell^*(v_n)$ where $\ell^* \in GL(V)$ is the dual linear transformation of ℓ, i.e. it has the property that

$$B(u, \ell(v)) = B(\ell^*(u), v).$$

By Lemma 7.11, $v_1, \dots, v_n$ is an R-basis for $D(M)$ and $\ell^*(v_1), \dots, \ell^*(v_n)$ is an R-basis for $D(N)$. We have therefore $[N : M] = \det(\ell)^{-1}R$ and $[D(M) : D(N)] = \det(\ell^*)R$. The result follows from the fact that

$$\det(\ell)\det(\ell^*) = 1 \text{ (exercise!)}.$$

□

Definition 7.13. The *discriminant* of the M is $\mathfrak{d}(M) = \mathfrak{d}(M/R) = [D_R(M) : M]_R$ the module index of M in its dual.

Proposition 7.14. (i) $\mathfrak{d}(N) = \mathfrak{d}(M)[M : N]^2$.

(ii) $\mathfrak{d}(M_\mathfrak{p}/R_\mathfrak{p}) = \mathfrak{d}(M/R)R_\mathfrak{p}$.

(iii) *If M is a free R-module with basis $x_1, \dots, x_n$ then $\mathfrak{d}(M)$ is the fractional ideal of R generated by* $\det(B(x_i, x_j))_{1\le i,j\le n}$.

Proof. (*i*) $\mathfrak{d}N = [D(N) : N] = [D(N) : D(M)][D(M) : M][M : N] = (\mathfrak{d}M)[M : N]^2$.

(*ii*) Follows from (ii) of the previous proposition.

(*iii*) Let $y_1, \dots, y_n$ be the dual basis. Let $\ell \in GL(V)$ such that $\ell(y_i) = x_i$. By Lemma 7.11 we have $[D(M) : M] = (\det \ell)R$. On the other hand,

$$\det(B(x_i, x_j))_{i,j} = \det(B(x_i, \ell(y_j)))_{i,j} = \det(\ell)\det B(x_i, y_j) = \det(\ell)$$

and the result follows.

□

Corollary 7.15. *If $M \supset N$, then $\mathfrak{d}M \mid \mathfrak{d}N$. If furthermore $\mathfrak{d}M = \mathfrak{d}N$, then $M = N$.*

Example 7.16. Take $R = \mathbb{Z}$ and $M = \mathbb{Z} \oplus 2\mathbb{Z}, N = 2\mathbb{Z} \oplus 3\mathbb{Z}$. Then $K = \mathbb{Q}, V = \mathbb{Q} \oplus \mathbb{Q}$. Take the dot product to be the bilinear form on V. Then $D(M) = \mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}$ and a linear transformation that takes $D(M)$ to M is given by

$$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

Thus $\mathfrak{d}(M) = 4\mathbb{Z}$. A K-basis for V contained in M is

$$u_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, u_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}.$$

The dual basis is

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1/2 \end{pmatrix},$$

which does span $D(M)$.

The matrix $(B(u_i,u_j))_{i,j}$ is

$$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$$

and its determinant indeed generates the fractional ideal $4\mathbb{Z} = \mathfrak{d}(M)$.

Similarly for N we get that $D(N) = \frac{1}{2}\mathbb{Z} \oplus \frac{1}{3}\mathbb{Z}$, the linear transformation that takes $D(N)$ to N is

$$\begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix}.$$

Thus $\mathfrak{d}(N) = 36\mathbb{Z}$. To get from M to N we use

$$\begin{pmatrix} 2 & 0 \\ 0 & 3/2 \end{pmatrix}$$

and so $[M : N] = 3\mathbb{Z}$. To get from $D(N)$ to $D(M)$ we use again the exact same matrix, which gives $[M : N] = [D(N) : D(M)] = 3\mathbb{Z}$. We also see that $\mathfrak{d}(M)[M : N]^2 = (4\mathbb{Z})(3\mathbb{Z})^2 = 36\mathbb{Z} = \mathfrak{d}(N)$.

Now assume $V = V_1 \oplus V_2$ ans suppose M_i, N_i span V_i for $i = 1, 2$. Denote $M = M_1 \oplus M_2$ and $N = N_1 \oplus N_2$.

Proposition 7.17. (i) *$[M : N] = [M_1 : N_1][M_2 : N_2]$.*

(ii) *If $B(V_1, V_2) = 0$, then $D(M) = D(M_1) \oplus D(M_2)$.*

(iii) *If $B(V_1, V_2) = 0$, then $\mathfrak{d}(M) = \mathfrak{d}(M_1)\mathfrak{d}(M_2)$.*

Proof. The first point is obvious, since the matrix that takes M to N will be a diagonal block matrix. For the next two, notice that $B(V_1, V_2) = 0$ implies that $B|_{V_i}$ is nondegenerate for $i = 1, 2$. □

Let S be a Dedekind domain containing R with quotient field L. We can view V as embedded in the L-vector space $W = V \otimes_K L$. The bilinear form B can uniquely be extended to an L-bilinear form B' on W that is again symmetric and nondegenerate. The S-module $M' = M \otimes_R S \subset W$ generated by M is finitely generated and it spans W. If M is free, then so is M'.

Proposition 7.18. (i) *$[M \otimes_R S : N \otimes_R S]_S = [M : N]_R \otimes_R S$.*

(ii) *$D_S(M \otimes_R S) = D_R(M) \otimes_R S$.*

(iii) *If $\mathfrak{d}(M \otimes_R S/S) = \mathfrak{d}(M/R)S$.*

Proof. The proof is immediate in the case of free R-modules. The general case is a bit more involved, but we will omit it here. □

8 Dedekind domains in field extensions

First, we go through a few preliminaries from commutative algebra.

Proposition 8.1. *If $A \subset B$ are commutative rings with B integral over A.*

(i) *Let $J \subset B$ an ideal and denote $I = J \cap A$. Then B/J is integral over A/I.*

(ii) *If S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof. (*i*) Any $x \in B$ satisfies a relation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_0, \ldots, a_{n-1} \in A$. Reducing this equation modulo J we see that $\bar{x} \in B/J$ is integral over A/I.

(*ii*) An element of $S^{-1}B$ is of the form $\frac{x}{s}$ with $x \in B, s \in S$. Dividing the equation above by s^n we get

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0$$

which shows that $\frac{x}{s}$ is integral over $S^{-1}A$.

□

Proposition 8.2. *Let $A \subset B$ be two integral domains such that B is integral over A. Then B is a field if and only if A is a field.*

Proof. ($\Longrightarrow$) Let $x \in A, x \neq 0$. Then there exists $y = x^{-1} \in B$ and this element is integral over A. Therefore there exist $a_0, \ldots, a_{n-1} \in A$ such that

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0.$$

Multiply both sides by x^{n-1} and get that

$$y = -\left(a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1}\right) \in A.$$

($\Longleftarrow$) Let $y \in B, y \neq 0$. This element is integral over A. Consider the integral dependence relation

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0,$$

with $a_0, \ldots, a_{n-1} \in A$ of smallest possible degree. Since B is an integral domain we must have $a_0 \neq 0$. Therefore

$$y\left(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1\right)(-a_0^{-1}) = 1,$$

so y is invertible in B. □

Corollary 8.3. *Let $A \subset B$ be commutative rings with B integral over A. Let J be a prime ideal of B and denote $I = J \cap A$. Then I is a prime ideal as well and $I \subset A$ is maximal if and only if $J \subset B$ is maximal.*

Proof. Both A/I and B/J are integral domains. By Proposition 8.1 B/J is integral over A/I. By Proposition 8.2, I maximal $\iff$ A/I field $\iff$ B/J field $\iff$ J maximal. □

Definition 8.4. Let $A \subset B$ be two commutative rings. We say that a prime ideal J of B *lies over (divides)* the prime ideal I of A if $J \cap A = I$. We write $J \mid I$.

Theorem 8.5. *Let $A \subset B$ be commutative rings with B integral over A. Let I be a prime ideal of A. Then there exists a prime ideal J of B such that $B \cap A = I$ (that lies above I).*

Proof. Let $S = A \setminus I$. This is a multiplicatively closed set in A and $S^{-1}A = A_I$ is a local ring with maximal ideal IA_I. By Proposition 8.1, $S^{-1}B$ is integral over A_I and the diagram

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\
A_I \arrow[r, hook] & S^{-1}B
\end{tikzcd}$$

is commutative. Let $\mathfrak{m}'$ be a maximal ideal of $S^{-1}B$. Then, by Corollary 8.3, $\mathfrak{m} = \mathfrak{m}' \cap I$ is a maximal ideal of A_I. But A_I is local, so $\mathfrak{m} = IA_I$ is the unique maximal ideal of A_I. Let $J = \beta^{-1}(\mathfrak{m}') \subset B$. Then J is prime and $J \cap A = \alpha^{-1}(\mathfrak{m}) = I$. □

Proposition 8.6. *Let $A \subset B$ be commutative rings and denote by C the integral closure of A in B. If S is a multiplicatively closed subset of A, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. Since C is integral over A, it follows from Proposition 8.1 that $S^{-1}C$ is integral over $S^{-1}A$. Now let $x \in S^{-1}B$ be an element integral over $S^{-1}A$. Then $x = \frac{b}{s}$ with $b \in B, s \in S$ and there exist $a_0, \ldots, a_{n-1} \in A, s_0, \ldots, s_{n-1} \in S$ such that

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s_0} = 0.$$

Clear denominators and get

$$s_0 \ldots s_{n-1} b^n + a_{n-1} s s_0 \ldots s_{n-2} b^{n-1} + \cdots + a_0 s^n s_1 \ldots s_{n-1} = 0,$$

so $s'b$ is integral over A where $s' = s_0 \ldots s_{n-1} \in S \subset A$. Thus $s'b \in C$ and $x = \frac{s'b}{s's} \in S^{-1}C$. □

Now we go back to our study of Dedekind domains. Throughout the rest of the section, R will be a Dedekind domain, K its quotient field, L/K a finite degree separable algebraic field extension and we denote by S the integral closure of R in L (i.e. the set of all elements of L that are integral over R). We know that S is a ring and that it is integrally closed in L.

Lemma 8.7. *If $\mathfrak{p}$ is a prime ideal of R, then $R_{\mathfrak{p}} \otimes_R S$ is the integral closure of $R_{\mathfrak{p}}$ in L.*

Proof. Follows directly from Proposition 8.6 using the fact that $R_{\mathfrak{p}} \otimes S \simeq R_{\mathfrak{p}}S = (R \setminus \mathfrak{p})^{-1}S$ via the isomorphism $R \otimes_R S \simeq S$.

□

Remark 8.8. *The trace map* $\mathrm{tr} = \mathrm{tr}_{L/K} : L \to K$ *defines a nondegenerate, symmetric* K*-bilinear form on* L *given by* $(\alpha, \beta) \to \mathrm{tr}_{L/K}(\alpha\beta)$.

Lemma 8.9. *If* $x \in L$ *is integral over* R*, then the (monic) minimal polynomial of* x *over* K *has coefficients in* R*. In particular,* $\mathrm{tr}(x), N_{L/K}(x) \in R$.

Proof. Whatever integral equation x satisfies, all its Galois conjugates satisfy it as well. So they are all integral over R. Thus the coefficients of the minimal polynomial of x over K are integral over R (since they are symmetric polynomials in x and its Galois conjugates). They are also elements of K and R is integrally closed. Thus all the coefficients of the minimal polynomial of x are actually in R, not just the trace and the norm. □

Proposition 8.10. *The ring* S *is a Dedekind domain, it is finitely generated as an* R*-module and it spans* L *over* K*. Every nonzero prime ideal* $\mathfrak{P}$ *of* S *lies over a nonzero prime ideal of* R *and there is a prime ideal of* S *lying over every nonzero prime ideal* $\mathfrak{p}$ *of* R.

Proof. By applying Lemma 8.7 for $\mathfrak{p} = 0$, we see that the integral closure of K in L, which is L itself, is equal to $K \otimes_R S$. Hence S generates L as a K-vector space. Any element $x \in L$ is algebraic over K and therefore it satisfies an equation of the form

$$a_n x^n + \cdots + a_0 = 0$$

with $a_0, \ldots, a_n \in R$. Multiplying by a_n^{n-1} we see that $b = a_n x$ is integral over R, hence $b \in S$. Thus given any basis of L over K we can multiply the basis elements by suitable elements of R and get a basis for L/K that actually consists of elements $u_1, \ldots, u_n \in S$. Take N the R-module spanned by $u_1, \ldots, u_n$. Then N is free of rank $n = \dim_K L$, it spans L and $N \subset S$. But then $D(N)$ is a free R-module, it spans L and $v_1, \ldots, v_n$ the dual basis to $u_1, \ldots, u_n$ with respect to the bilinear form $\mathrm{tr}(uv)$ is an R-basis of $D(N)$.
By Lemma 8.9 the traces of elements of S are in R. Thus $S \subset D(S)$. On the other hand, since $N \subset S$ we have $D(S) \subset D(N)$. Hence $S \subset D(N)$ is an R-submodule. But $D(N)$ is a finitely generated module over the noetherian ring R, so S is a finitely generated R-module. Hence S is a noetherian ring.
We already know that S is integrally closed. So it remains to prove that every nonzero ideal $\mathfrak{P} \subset S$ is maximal. We know that $\mathfrak{p} = R \cap \mathfrak{P}$ is a prime ideal of R. Let $b \in \mathfrak{P}, b \neq 0$. Take the minimal equation of b over K

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

As we have seen in Lemma 8.9, $a_0, \ldots, a_{n-1} \in R$. Therefore $a_0 \in R \cap \mathfrak{P} = R$ and since $a_0 \neq 0$, we have $\mathfrak{p} \neq 0$. Hence $\mathfrak{p}$ is a maximal ideal of R, Lemma 8.3 implies that $\mathfrak{P}$ is also maximal.

Now let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $\mathfrak{p}S$ is an integral ideal of S. If we prove that $\mathfrak{p}S \neq S$, then we know that $\mathfrak{p}S$ factors as a product of nonzero prime ideals of S, thus there exists a prime ideal of S that lies above $\mathfrak{p}$.
Assume by contradiction that $\mathfrak{p}S = S$. Then $\mathfrak{p}^{-1}S = \mathfrak{p}^{-1}(\mathfrak{p}S) = RS = S$, so $\mathfrak{p}^{-1} \subset S \cap K = R$. (Contradiction.)

□

Corollary 8.11. *Every discrete valuation v of a field K can be extended to a finite, separable extension L of K.*

Proof. Set R to be the valuation ring of v. Then $v_{\mathfrak{P}}$ extends v where $\mathfrak{P}$ is a prime ideal that lies above the valuation ideal of v. □

Note that if $I_1, I_2 \subset R$ ideals with $I_1 + I_2 = R$, then $I_1S + I_2S = S$. Thus the sets of prime ideals of S that lie above two distinct prime ideals of R are disjoint.

Corollary 8.12. *The map $I \mapsto IS$ is an injective homomorphism $\mathscr{I}(R) \to \mathscr{I}(S)$.*

Proposition 8.13. *For any number field K, the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is a Dedekind domain (called* the ring of integers *of K).*

9 Local fields: the finite residue case

Definition 9.1. A *local field* is a field K that is complete with respect to a discrete valuation.

Example 9.2. $\mathbb{Q}_p$ and $F((t))$, where F is any field, are both local fields.

Let K be a field and v a discrete valuation on K. Set $R = R_v \subset K$ the valuation ring of v inside K, $\mathfrak{p} = \mathfrak{p}_v \subset R$ the valuation ideal and by $k_v = R/\mathfrak{p}$ the residue field.
Denote by K_v the completion at v and by $S \subset K_v$ the valuation ring of v in the completion K_v. Let $\mathfrak{P} \subset S$ be the valuation ideal in S.

Proposition 9.3. *$S/\mathfrak{P} \simeq k_v$.*

So every field K endowed with a discrete valuation v can be embedded in a local field with respect to v with the same residue field.

Proposition 9.4. *Assume K is complete with respect to the discrete valuation v. Let R denote the valuation ring and $\mathfrak{p}$ the valuation ideal. Pick a* uniformizer *$\pi \in R$ (i.e. a generator of the maximal ideal $\mathfrak{p}$ of R.) Assume further that the residue field $k = R/\mathfrak{p}$ is finite. Then the ring R consists of elements*

$$\alpha = \sum_{j=0}^{\infty} a_j \pi^j = \lim_{n\to\infty} \sum_{j=0}^{n} a_j \pi^j$$

where a_j run independently through a set $\Sigma \subset R$ of representatives of $R/\mathfrak{p}$.

Proof. Exercise. □

Theorem 9.5. *Under the conditions of Proposition 9.4, R is compact in the valuation topology.*

Proof. Let $U_{ii\in I}$ be an open covering of R. Assume that it has no finite subcover. Let $\Sigma \subset R$ be a set of representatives for $R/\mathfrak{p} = k$. Then

$$R = \bigcup_{a\in\Sigma}(a+\mathfrak{p})$$

is a finite union. Hence there must exist $a_0 \in \Sigma$ such that $a_0+\mathfrak{p}$ is not covered by finitely many of the U_i's. Similarly, there exists $a_1 \in \Sigma$ such that $a_0 + a_1\pi + \pi^2 R$ is not covered by finitely many of the U_i's and so on. We get $a_0, a_1, \cdots \in \Sigma$ such that $a_0 + a_1\pi + \cdots + a_n\pi^n + \pi^{n+1}R$ is not covered by finitely many of the U_i's.

Let $\alpha = a_0 + a_1\pi + \ldots$ the limit of the infinite series in K. Then $\alpha \in R$ and therefore there exist $j \in I$ such that $\alpha \in U_j$. Since U_j is open, there exists $n > 0$ such that $\alpha + \pi^n R \in U_j$ (contradiction). □

Corollary 9.6. *Any local field with finite residue field is locally compact.*

Theorem 9.7. *Any local field K with finite residue field k is isomorphic to a finite extension of either $\mathbb{Q}_p$ or to $\mathbb{F}_q((t))$.*

Proof. Let $p = \operatorname{char} k$. There are two possibilities for K. It can either have $\operatorname{char} K = 0$ or $\operatorname{char} K = p$.

We first treat the cases when $\operatorname{char} K = p$. Then K is an $\mathbb{F}_p$-algebra. Since k is finite of characteristic p, it is of the form $k = \mathbb{F}_q = \mathbb{F}_p(\alpha)$. Let $m_\alpha \in \mathbb{F}_p[X]$ be the (monic) minimal polynomial of α over $\mathbb{F}_p$. Then $\deg m_\alpha = [k : \mathbb{F}_p]$. On the other hand, we can view $m_\alpha \in K[X]$. But m_α factors over the residue field k as

$$m_\alpha(X) = (X-\alpha)g(X).$$

By Hensel's Lemma we can lift this factorization to the ring $K[X]$ to $m_\alpha = (X-a)G(X)$ for some $a \in K$, $G(X) \in K[X]$ monic of degree $[k : \mathbb{F}_p] - 1$. Thus $K \supset \mathbb{F}_p(a) \simeq \mathbb{F}_q = k$ has a natural $\mathbb{F}_q$-algebra structure via the map $\alpha \mapsto a$. Then, by Proposition 9.4,

$$R = \left\{ \sum_{n\geq 0} a_n\pi^n ; a_n \in \mathbb{F}_p(a) \right\} \implies K \simeq \mathbb{F}_q((t)).$$

Now for the case when $\operatorname{char} K = 0$. Then $K \supset \mathbb{Q}$ and therefore there exits a prime p such that $v|_{\mathbb{Q}} = v_p$. Since K is complete it follows that $K \supset \mathbb{Q}_p$. On the other hand, both v and v_p have images isomorphic to $\mathbb{Z}$ and $\operatorname{im}(v) \supset \operatorname{im}(v_p)$. Thus $\operatorname{im}(v)/\operatorname{im}(v_p)$ is a finite group. Pick $\alpha_1, \ldots, \alpha_r \in K$ a complete set of representatives for this finite group. Pick a basis $\beta_1, \ldots, \beta_n$ of $k/\mathbb{F}_p$. Then

$$\alpha_i\beta_j, 1 \leq i \leq r, 1 \leq j \leq n$$

form a basis for $K/\mathbb{Q}_p$.

□

10 Tensor product of fields

Proposition 10.1. *Let $K \subset A, B$ be fields and assume that B/K is a separable extension of finite degree $[B : K] = n$. Then $C = A \otimes_K B$ is the direct sum of $r \leq n$ fields $L_1, \ldots, L_r$, each containing an isomorphic image of A and an isomorphic image of B.*

Proof. By the primitive element theorem, there exist $\beta \in B$ such that $B = K(\beta)$ with the minimal polynomial $f(X) \in K[X]$ of β over K separable of degree n. In particular, f is monic and irreducible over K. Then $1, \beta, \ldots, \beta^{n-1}$ form a basis of B over K. Therefore $C = A \otimes_K B = A[\bar{\beta}]$ with $1, \bar{\beta}, \ldots, \bar{\beta}^{n-1}$ linearly independent over A and $f(\bar{\beta}) = 0$. Although $f(X)$ is irreducible in $K[X]$, it might actually factor in $A[X]$. Consider its factorization in $A[X]$,

$$f(X) = \prod_{j=1}^{r} g_j(X),$$

where $g_j(X) \in A[X]$ irreducible and monic. Since $f(X)$ is separable, its factors $g_j(X)$ must be distinct. For each j pick a root β_j of $g_j(X)$ and set $L_j = A(\beta_j)$ and $\mu_j : A \otimes_K B = A[\bar{\beta}] \to L_j$ the map given by $h(\bar{\beta}) \mapsto h(\beta_j)$ for all $h \in A[X]$. Then L_j is a field and μ_j is a ring homomorphism. We put all these homomorphisms together and get the ring homomorphism

$$\mu = \mu_1 \oplus \cdots \oplus \mu_r : C = A \otimes_K B \to \bigoplus_{j=1}^{r} L_j.$$

We want to show that μ is an isomorphism. Note that both sides have the same dimension as A-vector spaces, hence it is enough to show that μ is injective. Start with an element in $\ker \mu$. This element lives in $A[\bar{\beta}]$, so it is of the form $h(\bar{\beta})$ for some $h(X) \in A[X]$. We have

$$0 = \mu(h(\bar{\beta})) = (\mu_1(h(\beta_1)), \ldots, \mu_r(h(\beta_r)))\,,$$

hence $h(X)$ must be divisible by $g_1(X), \ldots, g_r(X)$. Since they are distinct monic irreducible polynomials, their product $f(X)$ divides $h(X)$, so $h(\beta) = 0$. Thus $h(\bar{\beta}) = 0$.

Each field L_j contains a copy of A by construction. It remains to show that the ring homomorphisms $\lambda_j, 1 \leq j \leq r$, given by the composition

$$B \longrightarrow A \otimes_K B \xrightarrow{\mu_j} L_j$$

are injective. Since B is a field, this reduces to showing that $\lambda_j \neq 0$. Fortunately, $\lambda_j(1) = 1$, so this is trivially true.

□

Corollary 10.2. *Let $\alpha \in B$, $F(X) \in K[X]$ its minimal polynomial over K. Let $G_j \in A[X]$ be the minimal polynomial of $\lambda_j(\alpha) \in L_j$ over A, for all $1 \leq j \leq r$. Then*

$$F(X) = \prod_{j=1}^{r} G_j(X).$$

Proof. We show that both sides of the equality equal the minimal polynomial $T(X) \in A[X]$ of $\bar{\alpha}$ over A, where $\bar{\alpha} \in A \otimes_K B$ is the image of α via $B \to A \otimes_K B = C$.
Let $\omega_1, \dots, \omega_n$ be a basis for B/K. Then its image $\bar{\omega}_1, \dots, \bar{\omega}_n$ is a basis of C/A.

□

Corollary 10.3. *For $\alpha \in B$ we have*

$$N_{B/K}(\alpha) = \prod_{j=1}^{r} N_{L_j/A}(\alpha) \quad \mathrm{tr}_{B/K}(\alpha) = \sum_{j=1}^{r} \mathrm{tr}_{L_j/A}(\alpha).$$

11 Places of a field

Definition 11.1. A *place* of a field K is an equivalence class of generalized absolute values on K. A place is called *nonarchimedean* if it has a non-archimedean representative and *archimedean* otherwise. We write $|\cdot|_v$ for a representative of v. We also denote by K_v completion of K with respect to v.

As we have seen, each place has a representative that is an actual absolute value (i.e. it satisfies the triangle inequality. We have also seen that if two generalized absolute values are equivalent, they are both either archimedean or non-archimedean. So the definition above makes sense.

If the place v is non-archimedean, then it comes from a discrete valuation (that we denote also by v) on K and its representatives are of the form $x \mapsto \rho^{v_{\mathfrak{p}}(x)}$ where $\mathfrak{p}$ is the valuation ideal associated to the discrete valuation v and $0 < \rho < 1$.

Example 11.2.

- The places of $\mathbb{Q}$ are given by the primes p (nonarchimedean) and one archimedean place given by the usual absolute value.
- The places of $\mathbb{F}_q(t)$ are all non-archimedean: one for each irreducible monic polynomial and one given by $v_\infty(f/g) = \deg g - \deg f$.
- The places of $\mathbb{Q}(i)$ are given by the prime ideals of $\mathbb{Z}[i]$ (all non-archimedean) and one more place given by the square of the complex absolute value.

Definition 11.3. If L/K is an field extension, v is a place of K and w is a place of L, we say that $w \mid v$ (*divides* or *lies above*) if w and v induce the same topology on K. Note that in this case, there exist representatives $|\cdot|$ of v and $\|\cdot\|$ of w such that $\|\alpha\| = |\alpha|$ for all $\alpha \in K$.

Theorem 11.4. *Assume K is a field endowed with a generalized absolute value $|\cdot|$ and that it is complete in the induced topology. Let L/K be a field extension of degree $[L : K] = n < \infty$. Then there is a unique extension of $|\cdot|$ to L, namely*

$$\|\beta\| = |N_{L/K}(\beta)|^{1/n}. \tag{11.1}$$

That is, for every place v of K with $K_v = K$, there exists a unique place w of L such that $w|v$.

Proof. First note that for $\alpha \in K$ we have indeed

$$\|\alpha\| = |\alpha^n|^{1/n} = |\alpha|.$$

Uniqueness: The field L can be regarded as a K-vector space and then any extension $\|\cdot\|$ is a vector space pseudonorm (i.e. it satisfies the generalized triangle inequality instead of the actual triangle inequality) on L compatible with $|\cdot|$. Since K is complete and L/K is finitely dimensional, it follows that any two extensions $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent as vector space pseudonorms (the concept is the same as for actual norms; the proof that any two pseudonorms on a finite dimensional vector space are equivalent is the same as for bonafide norms). Since they are equivalent vector space pseudonorms, they induce the same topology on L. This makes them equivalent as generalized absolute values, i.e. there exists some constant $c > 0$ such that $\|\cdot\|_1 = \|\cdot\|_2^c$. But

$$\|\alpha\|_1 = |\alpha| = \|\alpha\|_2 \quad \forall\, \alpha \in K,$$

so $c = 1$.

Formula: Fix $\beta \in L$ Then we have $K \subset K(\beta) \subset L$ and $N_{L/K}(\beta) = N_{K(\beta)/K}(\beta)^{[L:K(\beta)]}$. Hence it is enough to verify (11.1) for normal extensions.

Assume L/K is a normal extension. Let $\sigma \in \mathrm{Gal}(L/K)$. Then $\|\beta\|_\sigma = \|\sigma(\beta)\|$ also defines an extension of $|\cdot|$ to L. By uniqueness we have $\|\sigma(\beta)\| = \|\beta\|$ for any $\beta \in L$ and any $\sigma \in \mathrm{Gal}(L/K)$. Therefore

$$|N_{L/K}(\beta)| = \|N_{L/K}(\beta)\| = \left\| \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) \right\| = \prod_{\sigma \in \mathrm{Gal}(L/K)} \|\sigma(\beta)\| = \|\beta\|^n.$$

Existence: We will prove this only in the case when K is locally compact (all local fields, as well as $\mathbb{R}$ and $\mathbb{C}$, are locally compact) which is the only case of interest in this course. The proof in the general case can be found in Emil Artin's *Algebraic numbers and algebraic functions* (chapter 2, sections 1-4). It uses Hensel's lemma for the non-archimedean case and an approximation of Cauchy's residue theorem to prove that the only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$.

The function defined by (11.1) takes values in $\mathbb{R}_{\geq 0}$ and $\|\beta\| = 0 \iff N_{L/K}(\beta) = 0 \iff \beta = 0$. It is equally clear that $\|\beta\gamma\| = \|\beta\|\|\gamma\|$ for all $\beta, \gamma \in L$ (the norm is multiplicative). It remains to show that $\|\cdot\|$ satisfies the generalized triangle inequality, i.e. that there exist a constant $C > 0$ such that $\|1 + \beta\| \leq C$ whenever $\|\beta\| \leq 1$.
Let $\|\cdot\|_0$ be any K-vector space norm on L.
We will use the following fact from topology: if K is locally compact, then for any $0 \leq c_1 \leq c_2$ the set $A = \{x \in L; c_1 \leq \|x\|_0 \leq c_2\}$ is compact.
Fix an element $\alpha \in K$ with $|\alpha| > 1$. (If such an element does not exist, then $|\cdot|$ is trivial and (11.1) defines the trivial norm on L.) Choose $c_1 = 1$ and $c_2 = |\alpha|$. Since $\|\cdot\|$ is a continuous nonzero function on the L with its (unique) K-vector space topology, so it is bounded on A

and it attains both its maximum and its minimum. That is, there exist $M, m > 0$ such that $0 < m \leq \|\beta\| \leq M$ for all $x \in A$. Let $\beta \in L, \beta \neq 0$. Then there exists $r \in \mathbb{Z}$ such that

$$0 < c_2^r \leq \|\beta\|_0 \leq c_2^{r+1}. \tag{11.2}$$

This implies that $\alpha^{-r}\beta \in A$ and therefore

$$0 < mc_2^r \leq \|\beta\| \leq Mc_2^r. \tag{11.3}$$

Dividing (11.3) by (11.2) we get that

$$0 < \frac{m}{c_2} \leq \frac{\|\beta\|}{\|\beta\|_0} \leq M \quad \forall \beta \in L, \beta \neq 0.$$

Assume $0 < \|\beta\| \leq 1$. The above inequality implies that

$$0 < \|\beta\|_0 \leq \frac{c_2}{m}$$

and therefore

$$\|1+\beta\| \leq M\|1+\beta\|_0 \leq M(\|1\|_0 + \|\beta\|_0) \leq M\left(\|1\|_0 + \frac{c_2}{m}\right) \overset{\text{def}}{=} C > 0.$$

□

Corollary 11.5. *A finite extension L of a complete field $(K, |\cdot|)$ is complete with respect to the extension of $|\cdot|$. The topology on L is that of a finitely dimensional K-vector space.*

Combining the above result with Proposition 8.10, we obtain the following result about extensions of discrete valuation rings.

Corollary 11.6. *Let R be a discrete valuation ring and K its quotient field. Assume K is complete with respect to the discrete valuation induced by R and let L/K be a finite separable extension. Denote by S the integral closure of R in L. Then S is a discrete valuation ring and L is complete.*

If K is *not* complete with respect to the place v, the picture is more complicated.

Theorem 11.7. *Let L/K be a separable finite extension of degree n. Assume v is a place K and denote by K_v the completion of K at v. Then there are $w_1, \ldots, w_r, r \leq n$ distinct places of L above v and*

$$K_v \otimes_K L = \bigoplus_{j=1}^{r} L_{w_j} = \bigoplus_{w|v} L_w \tag{11.4}$$

algebraically and topologically (where the direct sum has the product topology).

Proof. We already know that $K_v \otimes_K L = \bigoplus_{j=1}^{r} L_i$ with $r \leq n$ and L_j/K_v finite field extensions. Hence for each j there exist a unique place w'_j of L_j such that $w'_j \mid v$ and furthermore L_j is complete with respect to w'_j. Pick $\| \cdot \|'_j$ a representative of w'_j.
On the other hand we know (from the proof of Proposition 10.1) that the ring homomorphisms $\lambda_j : L \to K_v \otimes_K L \to L_j$ are injective. Hence we get a place w_j of L that lies above v by taking the equivalence class of $\|x\|_j = \|\lambda_j(x)\|'_j, x \in L$.
Moreover, $L \simeq \lambda_j(L)$ is dense in L_j with respect to w_j because $L = K \otimes_K L$ is dense in $K_v \otimes_K L$. Hence $L_j = L_{w_j}$. We still need to prove two things: that the places w_j are distinct and that they are the only places of L that lie above v. Let w be any place of L such that $w \mid v$. Pick $\| \cdot \|$ a representative of w and $| \cdot |$ a representative of v such that they are absolute values and $\| \cdot \|$ extends $| \cdot |$. Then $\| \cdot \|$ extends by continuity to a function $f : K_v \otimes_K L \to \mathbb{R}_{\geq 0}$. Again by continuity the function f satisfies

$$f(xy) = f(x)f(y), \quad f(x+y) \leq f(x) + f(y) \quad \forall\, x, y \in K_v \otimes_K L.$$

Consider f_j the restriction of f to L_j. Assume that there exists $\beta \in L_j$ such that $f_j(\beta) \neq 0$. Then for every $\alpha \in L_{w_j}$, $\alpha \neq 0$ we have

$$f_j(\alpha) f_j(\alpha^{-1}\beta) = f_j(\beta) \neq 0,$$

and so $f_j(\alpha) \neq 0$.

Therefore f_j is either identically 0 or an absolute value on L_{w_j}. On the other hand, we cannot have f_i and f_j both not identically 0 for some $i \neq j$. This is because

$$(0, \dots, \alpha_i, \dots, 0) \cdot (0, \dots, \alpha_j, \dots, 0) = (0, \dots, 0) \implies f_i(\alpha_i) f_j(\alpha_j) = 0\, \forall\, \alpha_i \in L_i, \alpha_j \in L_{w_j}.$$

Hence f gives rise to a place for exactly one L_{w_j} and it clearly extends $| \cdot |$ (since f extends $\| \cdot \|$). Thus there exists a unique j_0 such that $w = w_{j_0}$.

It remains to show that (11.4) is a topological homomorphism. Define

$$\| \cdot \|_0 : \bigoplus L_{w_j} \to \mathbb{R}_{\geq 0} \quad \|(\beta_1, \dots, \beta_r)\|_0 = \max\{\|\beta\|_j; 1 \leq j \leq r\}.$$

Then $\| \cdot \|_0$ is a K_v-vector space norm on $\bigoplus L_{w_j}$ and it induces the product topology. On the other hand, since K_v is complete, any two norms on $\bigoplus L_{w_j}$ are equivalent, and therefore $\| \cdot \|_0$ induces the tensor product topology on $K_v \otimes_K L$.

□

Corollary 11.8. *Let $L = K(\beta)$ for some algebraic element β over K. Let $f(X) \in K[X]$ be the minimal polynomial of β over K. Suppose $f(X)$ factors over the completion $\hat{K}$ as*

$$f(X) = \prod_{j=1}^{r} g_j(X)$$

with $g_j(X) \in \hat{K}[X]$ monic and irreducible. Then $L_j = \hat{K}(\beta_j)$ where β_j is a root of $g_j(X)$.

Combining the results from this section with Proposition 8.10, we obtain the following results about extensions of discrete valuation rings.

Corollary 11.9. *Suppose R is a discrete valuation ring and its quotient field K is complete in the induced topology. Let L/K be a finite separable extension and denote by S the integral closure of R in S. Then S is also a discrete valuation ring and L is complete. In particular, any finite separable extension of a local field is also a local field.*

Proof. The extension of the discrete valuation on K to L is unique. □

Corollary 11.10. *Let R be a discrete valuation ring, K its quotient field. Denote by K_v the completion of K with respect to the corresponding discrete valuation and by $\mathfrak{p}$ the valuation ideal. Let L/K be a finite extension of degree n and S the integral closure of R in L.*

(i) S has finitely many nonzero prime ideals $\wp_1, \ldots, \wp_r, r \leq n$ and they all lie above $\mathfrak{p}$.

(ii) Let $L_j = L_{\wp_j}$ the completion of L with respect to the discrete valuation induced by $\wp_j$, $1 \leq j \leq r$. Then

$$L \otimes_K K_v = \bigoplus_{j=1}^{r} L_j$$

as algebras and topological K_v-vector spaces.

(iii) Let R_v be the valuation ring in K_v and S_j the valuation ring of $L_j, 1 \leq j \leq r$. Then

$$R_v \otimes_R S = \bigoplus_{j=1}^{r} S_j.$$

Proof. (i, ii) Follow directly from Theorem 11.7.

(iii) $\oplus S_j$ is the integral closure of R_v in $\oplus L_j$. Hence $R_v \otimes_R S \subset \oplus S_j$.
On the other hand, $R_v \otimes_R S$ is complete, and therefore closed in $\oplus L_j$. So it will be enough to show that S is dense in $\oplus S_j$. The weak approximation theorem implies that L is dense in $\oplus L_j$. Therefore $\oplus S_j$ is the closure of $\oplus S_j \cap L$. The minimal polynomial of an element $x \in \oplus S_j \cap L$ over K_v has coefficients in R_v. But it is also the minimal polynomial of x over K, and therefore its coefficients lie in $R_v \cap K = R$. So x is integral over R, and this means that $x \in S$. □

12 Weak approximation theorem

Theorem 12.1 (Weak approximation). *Let $| \cdot |_n$ with $1 \leq n \leq N$ be nontrivial non-equivalent generalized absolute values on a field F. For each n denote by F_n the topological space induced by $| \cdot |_n$ on F. Then the image Δ of F in the product topological space*

$$X = \prod_{n=1}^{N} F_n$$

is dense in X. In other words, given $\alpha_n \in F, 1 \le n \le N$ and $\varepsilon > 0$ there exist $a \in F$ such that

$$|a - \alpha_n|_n < \varepsilon \text{ for all } 1 \le n \le N.$$

Proof. It is enough to find $x_n \in F$ such that $|x_n|_n > 1$ and $|x_n|_m < 1$ when $m \neq n$. If we do manage to find these elements, then we can construct the following sequences:

$$\frac{1}{1+(x_n)^{-r}} \xrightarrow{|\cdot|_n} 1 \quad \frac{1}{1+(x_n)^{-r}} \xrightarrow{|\cdot|_m} 0 \text{ for } m \neq n.$$

Pick a sufficiently large r (this depends only on ε and $M = \max\{|\alpha_n|_m; 1 \le m, n \le N\}$) and set

$$a = \sum_{n=1}^{N} \frac{1}{1+(x_n)^{-r}} \alpha_n \in F.$$

By symmetry it is sufficient to find $x = x_1$ such that $|x|_1 > 1$ and $|x|_n < 1$ for $2 \le n \le N$.

We induct on $N \ge 2$.

For $N = 2$: since $|\cdot|_1$ and $|\cdot|_2$ are not equivalent, there exists $a, b \in F$ such that

$$|a|_1 < 1, \quad |a|_2 \ge 1, \quad |b|_1 \ge 1, \quad |b|_2 < 1.$$

Set $x = ba^{-1}$. Then $|x|_1 > 1$ and $|x|_2 < 1$ as required.

Induction step: by the induction hypothesis, there exists $y \in F$ such that $|y|_1 > 1$ and $|y|_n < 1$ for $2 \le n \le N-1$. By the case $N = 2$ there exists $z \in F$ such that $|z|_1 > 1$ and $|z|_N < 1$. Then we can find $r \in \mathbb{Z}_{>0}$ sufficiently large so that

$$x = \begin{cases} y & \text{if } |y|_N < 1 \\ y^r z & \text{if } |y|_N = 1 \\ \dfrac{1}{1+y^{-r}} z & \text{if } |y|_N > 1 \end{cases}$$

does the job.

□

Remark 12.2. *If $F = \mathbb{Q}$ and we take a bunch of p-adic valuations, the weak approximation theorem resembles the Chinese Remainder Theorem. But the true generalization of CRT is the* strong *approximation theorem that will be discussed next quarter.*

13 Ideal norms

We are again in the following situation: R is a Dedekind domain, K is its quotient field, L/K is a finite separable field extension and S is the integral closure of R in L. We will study a number of concepts associated with the embedding of R in S. In each case our strategy will be to reduce to the complete local case.

A fractional ideal J of S is finitely generated over S, and therefore over R. We also know that there exists $a \in S, a \neq 0$ such that $aJ \subset S$. Thus J contains a K-basis of L, i.e. it spans L over K. So the we can make the following definition.

Definition 13.1. The *ideal norm* of J in L/K is $N_{L/K}(J) = [S : J]_R$ (a fractional ideal of R).

The connection with the element norm is given by the following result.

Proposition 13.2. *If $a \in L^\times$, then*

$$N_{L/K}(aS) = N_{L/K}(a)R.$$

Proof. $x \mapsto ax$ is a K-linear automorphism of L that maps S to aS. Therefore $N_{L/K}(aS)$ is the fractional ideal of R generated by its determinant, $N_{L/K}(a)$.

□

Remark 13.3. *If $R = \mathbb{Z}$, then $N_{L/K}(J)$ is just the ideal of $\mathbb{Z}$ generated by $\#S/J$.*

For every nonzero prime ideal $\mathfrak{p}$ of R we will denote by $K_\mathfrak{p}$ the completion of K with respect to the discrete valuation $v_\mathfrak{p}$ and by $\hat{R}_\mathfrak{p}$ its valuation ring. Similarly, we define $L_\wp$ and $\hat{S}_\wp$ for a nonzero prime ideal $\wp$ of S.

Proposition 13.4. *If J is a fractional ideal of S, then*

$$N_{L/K}(J)\hat{R}_\mathfrak{p} = \prod_{\wp|\mathfrak{p}} N_{L_\wp/K_\mathfrak{p}}(J\hat{S}_\wp).$$

Proof. Given the fact that the module index is defined via localizations and in view of Lemma 8.7, it is enough to prove the result when $R = R_\mathfrak{p}$ is a discrete valuation ring. The result follows from Corollary 11.10 and Propositions 7.17 and 7.18. That is,

$$N_{L/K}(J)\hat{R}_\mathfrak{p} = [S : J]_R \otimes \hat{R}_\mathfrak{p} \overset{7.18}{=} \left[S \otimes \hat{R}_\mathfrak{p} : J \otimes \hat{R}_\mathfrak{p}\right]_{\hat{R}_\mathfrak{p}} \overset{11.10}{=} \left[\bigoplus_{\wp|\mathfrak{p}} \hat{S}_\wp : \bigoplus_{\wp|\mathfrak{p}} J \otimes_R \hat{S}_\wp\right]_{\hat{R}_\mathfrak{p}}.$$

By Proposition 7.17, this equals

$$\prod_{\wp|\mathfrak{p}} [\hat{S}_\wp : J\hat{S}_\wp]_{\hat{S}_\wp} = \prod_{\wp|\mathfrak{p}} N_{L_\wp/K_\mathfrak{p}}(J\hat{S}_\wp).$$

□

Corollary 13.5. *The ideal norm $N_{L/K}$ defines a group homomorphism $N_{L/K} : \mathscr{I}(S) \to \mathscr{I}(R)$.*

Proof. By Proposition 13.4 and Corollary 6.12, the proof reduces to the case when R is a dvr and K is complete. Then S is also a dvr (Corollary 11.9), and therefore all its fractional ideals are principal. The result follows from Proposition 13.2 and the multiplicativity of the norm on elements. □

The following corollaries follow along the same lines.

Corollary 13.6. *For $I \in \mathscr{I}(R)$ we have $N_{L/K}(IS) = I^{[L:K]}$.*

Corollary 13.7. *If $L \supset F \supset K$ are finite separable field extensions, and J is a fractional ideal of L, then*

$$N_{L/K}(J) = N_{F/K}\left(N_{L/F}(J)\right).$$

The dual $D_R(S)$ of S with respect to $\mathrm{tr} = \mathrm{tr}_{L/K}$ has a natural structure of S-module. We also know, by Propositions 7.12 and 8.10, that it is finitely generated as an R-module, and thus it is finitely generated over S. Clearly $D_R(S) \supset S$, so its inverse is an integral ideal of S.

Definition 13.8. The *different* of L/K is $\mathfrak{D} = \mathfrak{D}_{L/K} = D_R(S)^{-1} \subset S$. The *discriminant* L/K is $\mathfrak{d} = \mathfrak{d}_{L/K} = \mathfrak{d}(S/R) = [D_R(S) : S]_R \subset R$ integral ideal of R.

Remark 13.9.

$$\mathfrak{d} = [D_R(S) : S] = [S : D_R(S)]^{-1} = N_{L/K}\left(D_R(S)\right)^{-1} = N_{L/K}\left(\mathfrak{D}^{-1}\right)^{-1} = N_{L/K}(\mathfrak{D}).$$

Proposition 13.10. *In the notation of Proposition 13.4,*

(i) $\mathfrak{D}(S/R)\hat{S}_{\wp} = \mathfrak{D}(\hat{S}_{\wp}/R_{\mathfrak{p}})$.

(ii) $\mathfrak{d}(S/R)\hat{R}_{\mathfrak{p}} = \prod_{\wp|\mathfrak{p}} \mathfrak{d}(\hat{S}_{\wp}/\hat{R}_{\mathfrak{p}})$.

Next we want to establish a connection between the discriminant $\mathfrak{d}(S/R)$ and the discriminant of an integral generator of L. Choose $\alpha \in S$ such that $L = K[\alpha]$ and let $g \in K[X]$ the minimal polynomial of α over K. In this case, the ring $R[\alpha]$ spans L and is a free R-module with basis $1, \alpha, \ldots, \alpha^{n-1}$.

Proposition 13.11. *In this situation, we have*

(i) $D_R\left(R[\alpha]\right) = \frac{1}{g'(\alpha)}R[\alpha]$;

(ii) $\mathfrak{d}\left(R[\alpha]/R\right) = N_{L/K}\left(g'(\alpha)\right)R$;

(iii) $R[\alpha] = S \iff \mathfrak{D}(S/R) = g'(\alpha)S$.

Proof. Denote $A = R[\alpha]$.

(ii) By Proposition 7.14 we know that

$$\mathfrak{d}(A) = \det(\mathrm{tr}(\alpha^{i+j}))_{i,j}R.$$

But linear algebra teaches us that

$$\det(\mathrm{tr}(\alpha^{i+j}))_{i,j} = \pm N_{L/K}(g'(\alpha))$$

and therefore $\mathfrak{d}(A) = N_{L/K}(g'(\alpha))R$.

(i) We claim that $\mathrm{tr}_{L/K}\left(\frac{\alpha^m}{g'(\alpha)}\right) \in R$ for all $0 \le m \le n-1$. Thus

$$\frac{1}{g'(\alpha)}A \subset D_R(A).$$

On the other hand,

$$[D(A) : A] = \mathfrak{d}(A) = N_{L/K}(g'(\alpha))R = \left[\frac{1}{g'(\alpha)}A : A\right]$$

and the result follows.

It remains therefore to prove the claim. For this we will use the following polynomial identity of Euler:

$$(13.1) \qquad \sum_{j=1}^{n} \frac{\alpha_j^m}{g'(\alpha_j)} \, \frac{g(X)}{X - \alpha_j} = X^m, 0 \le m \le n-1,$$

where $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ are the roots of $g(X)$. (Exercise!) Then

$$\mathrm{tr}_{L/K}\left(\frac{\alpha^m}{g'(\alpha)}\right) = \sum_{j=1}^{n} \frac{\alpha_j^m}{g'(\alpha_j)}$$

is the coefficient of X^{n-1} in (13.1). It is therefore equal to either 0 or 1, so an element of R.

(iii) If $A = S$, then $\mathfrak{D}(S/R) = \mathfrak{D}(A) = D(A)^{-1} = g'(\alpha)A = g'(\alpha)S$.

For the reverse implication, assume that $\mathfrak{D}(S/R) = g'(\alpha)S$. Then

$$D(A) \supset D(S) = \mathfrak{D}(S)^{-1} = \frac{1}{g'(\alpha)}S \supset \frac{1}{g'(\alpha)}A = D(A).$$

Thus $D(A) = D(S)$ and therefore

$$A = D(D(A)) = D(D(S)) = S.$$

□

Proposition 13.12 (Tower formula)**.** *If $L \supset F \supset K$ are finite separable field extensions, and if T is the integral closure of R in F, then*

(i) $\mathfrak{D}(S/R) = \mathfrak{D}(S/T)\mathfrak{D}(T/R)$;

(ii) $\mathfrak{d}(S/R) = \mathfrak{d}(T/R)^{[L:F]}\, N_{F/K}\left(\mathfrak{d}(S/T)\right).$

Proof. Let $m = [L : F]$.

(i) We will actually prove that $\mathfrak{D}(S/R)^{-1} = \mathfrak{D}(S/T)^{-1}\mathfrak{D}(T/R)^{-1}$.

This is equivalent to

$$D_R(S) = D_T(S)D_R(T).$$

By the transitivity of the trace we have, for every $x \in L$,

$$\mathrm{tr}_{L/K}(Sx) = \mathrm{tr}_{F/K}\left(\mathrm{tr}_{L/F}(Sx)T\right).$$

Hence

$$x \in D_R(S) \iff \mathrm{tr}_{L/K}(Sx) \subset R \iff \mathrm{tr}_{L/K}(Sx) \subset D_R(T) = \mathfrak{D}(T/R)^{-1},$$

which is equivalent to

$$\mathrm{tr}_{L/K}(Sx\mathfrak{D}(T/R)) \subset T \iff x\mathfrak{D}(T/R) \subset D_T(S) \iff x \in D_R(T)D_T(S).$$

(ii) Follows by taking $N_{L/K}$ in (i).

□

14 Ramification

Let $R_1 \subset R_2 \subset R_3$ be Dedekind domains with quotient fields K_1, K_2, K_3. Assume that $\mathfrak{p}_i$ is a nonzero prime ideal of R_i and that $\mathfrak{p}_2 \cap R_1 = \mathfrak{p}_1$. Then the residue field $k_1 = R_1/\mathfrak{p}_1$ is embedded naturally in the residue field $k_2 = R_2/\mathfrak{p}_2$.

Definition 14.1. The degree $[k_2 : k_1] = f(\mathfrak{p}_2/\mathfrak{p}_1) \leq \infty$ is called the *residue class degree* or the *inertia degree.* The *ramification index* is $e(\mathfrak{p}_2/\mathfrak{p}_1) = v_{\mathfrak{p}_2}(\mathfrak{p}_1 R_2)$.

Note that

$$v_{\mathfrak{p}_2}|K_1^\times = e(\mathfrak{p}_2/\mathfrak{p}_1)v_{\mathfrak{p}_1}, i.e. \quad \mathfrak{p}_2^e \| \mathfrak{p}_1. \tag{14.1}$$

Proposition 14.2. *In the obvious notation,*

$$e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2)e(\mathfrak{p}_2/\mathfrak{p}_1) \quad \textit{and} \quad f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2)f(\mathfrak{p}_2/\mathfrak{p}_1).$$

Proposition 14.3. *Let R be a Dedekind domain, K its quotient field and $\mathfrak{p}$ a nonzero prime ideal of R. Let $v = v_\mathfrak{p}$ the discrete valuation induced by $\mathfrak{p}$ and $\mathfrak{p}_v$ the valuation ideal in the completion K_v. Then*

$$e(\mathfrak{p}_v/\mathfrak{p}) = f(\mathfrak{p}_v/\mathfrak{p}) = 1.$$

Proof. The local ring $R_\mathfrak{p} \subset K$ is the valuation ring of v. Then Proposition 6.7 tells us that $e(\mathfrak{p}R_\mathfrak{p}/\mathfrak{p}) = 1$. On the other hand, Proposition 5.12, $e(\mathfrak{p}_v/\mathfrak{p}R_\mathfrak{p}) = 1$. We get that $(\mathfrak{p}_v/\mathfrak{p}) = 1$ by multiplicativity.

Every element of $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is of the form $\frac{x}{y}$ with $x, y \in R/\mathfrak{p}$. Hence

$$R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = R/\mathfrak{p} \implies f(\mathfrak{p}R_\mathfrak{p}/\mathfrak{p}) = 1.$$

On the other hand, $R_\mathfrak{p}$ is dense in the valuation ring R_v of K_v. Hence the image of $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is dense in the discrete group $R_v/\mathfrak{p}_v$. Therefore $f(\mathfrak{p}_v/\mathfrak{p}R_\mathfrak{p}) = 1$ and the result follows again by multiplicativity.

□

Corollary 14.4.

$$f(\mathfrak{p}_2/\mathfrak{p}_1) = f(\mathfrak{p}_{v_2}/\mathfrak{p}_{v_1}) \quad \textit{and} \quad e(\mathfrak{p}_2/\mathfrak{p}_1) = e(\mathfrak{p}_{v_2}/\mathfrak{p}_{v_1}).$$

It is clear now that differents, discriminants, ramification indices, residue class indices and ideal norms can be described locally in terms of completions. For this reason our strategy will be to prove results about these concepts for the case when R is a dvr and K is complete in the valuation topology. This situation is inherited by finite separable extensions (Corollary 11.6). These results then lift to the global situation.

We assume that the residue class field extensions are separable.

Proposition 14.5. *If $\mathfrak{p}$ is a nonzero prime ideal of R and $\wp$ is a prime ideal of S lying over $\mathfrak{p}$, then*

$$e(\wp/\mathfrak{p})f(\wp/\mathfrak{p}) = [L_\wp : K_\mathfrak{p}].$$

Proof. It is enough to prove this in the case when R is a dvr with maximal ideal $\mathfrak{p}$ and $K = K_\mathfrak{p}$ is complete in the valuation topology. Then, by Corollary 11.6, S is also a dvr with maximal ideal $\wp$ and $L = L_\wp$ is complete. We have $\mathfrak{p}S = \wp^e$ where $e = e(\wp/\mathfrak{p})$. Then $S/\mathfrak{p}S$ is a k-vector space and it has a sequence of quotient spaces all isomorphic (by Propositon 5.24) to $S/\wp$:

$$S/\wp, \wp/\wp^2, \ldots, \wp^{e-1}/\wp^e.$$

By definition, $\dim_k S/\wp = f$, hence $\dim_k S/\mathfrak{p}S = ef$. On the other hand, we know that S is a free R-module of rank $[L : K]$, hence $\dim_k S/\mathfrak{p}S = [L : K]$.

□

Proposition 14.6. *If $\mathfrak{p}$ is a nonzero prime ideal of R and $\wp_1, \ldots, \wp_r$ are all the prime ideals of S lying above $\mathfrak{p}$, then*

$$\mathfrak{p}S = \wp_1^{e_1} \ldots \wp_r^{e_r}$$

and

$$\sum_{j=1}^{r} e_j f_j = [L : K],$$

where $e_j = e(\wp_j/\mathfrak{p})$ and $f_j = f(\wp_j/\mathfrak{p})$.

Proof. The very definition of the ramification index e_j implies that $\mathfrak{p}S = \wp_1^{e_1} \ldots \wp_r^{e_r}$. For the second part, recall that

$$L \otimes K_{\mathfrak{p}} = \bigoplus_{j=1}^{r} L_{\wp_j}.$$

We have from the previous proposition that $e_j f_j = [L_{\wp_j} : K_{\mathfrak{p}}]$ and therefore

$$\sum_{j=1}^{r} e_j f_j = \dim_{K_{\mathfrak{p}}} L \otimes K_{\mathfrak{p}} = \dim_K L = [L : K].$$

□

Denote by $U_{\mathfrak{p}}$ the unit group of $K_{\mathfrak{p}}$ and $U_{\wp}$ the unit group of $L_{\wp}$. We have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & U_{\mathfrak{p}} \arrow[r] \arrow[d] & K_{\mathfrak{p}}^{\times} \arrow[r, "v_{\mathfrak{p}}"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, "e"] & 0 \\
0 \arrow[r] & U_{\wp} \arrow[r] & L_{\wp}^{\times} \arrow[r, "v_{\wp}"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where the last downward arrow is given by the multiplication by $e = e(\wp/\mathfrak{p})$.

Proposition 14.7. *The norm map yields a commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & U_{\wp} \arrow[r] \arrow[d] & L_{\wp}^{\times} \arrow[r, "v_{\wp}"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & U_{\mathfrak{p}} \arrow[r] & K_{\mathfrak{p}}^{\times} \arrow[r, "v_{\mathfrak{p}}"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where the last downward arrow is given by the multiplication by $f = f(\wp/\mathfrak{p})$. That is,

$$v_{\mathfrak{p}}(N_{L_{\wp}/K_{\mathfrak{p}}}(x)) = f v_{\wp}(x) \text{ for all } x \in L_{\wp}$$

and

$$N_{L_{\wp}/K_{\mathfrak{p}}}(\wp) = \mathfrak{p}^f.$$

Proof. Boils down to $N_{L/K}(\alpha) = \alpha^{[L:K]}$ for all $\alpha \in K$. That is, the left hand side of the diagram obviously commutes since the norm of a unit is a unit. There exists a group endomorphism of $\mathbb{Z}$ that makes the right hand side of the diagram commute as well. Since it is an endomorphism of $\mathbb{Z}$ is given by the multiplication by a certain integer. In order to determine the integer, we take $x \in K_{\mathfrak{p}}$ and apply the various transformations to it. Then

$$v_{\mathfrak{p}}(N(x)) = v_{\mathfrak{p}}\left(x^{[L_{\wp}:K_{\mathfrak{p}}]}\right) = [L_{\wp} : K_{\mathfrak{p}}]v_{\mathfrak{p}}(x) = efv_{\mathfrak{p}}(x) = fv_{\wp}(x)$$

by (14.1). The last equation follows from the fact that the equality holds for the valuation ideals in the completions. □